ICANN78 | Reunión General Anual – ccNSO: actualización para la comunidad del Comité Permanente de Uso Indebido del DNS
Miércoles, 25 de octubre de 2023 – 1:30 a 3:30 HAM

CLAUDIA RUIZ: Comencemos con la grabación. Hola y bienvenidos a la sesión sobre uso indebido del DNS, herramientas y mediciones, de la ccNSO. Soy Claudia Ruiz y estoy aquí con Andrea Glandon y con Bart Boswinkel. Seremos los coordinadores de participación en esta sesión. Tengan en cuenta que esta sesión se rige por los estándares de comportamiento esperado de la ICANN. En la sesión las preguntas o comentarios que se formulen en el chat solo se leerán en voz alta si están escritos de la manera correcta como se indicó en el chat. Leeré las preguntas y los comentarios en voz alta durante el espacio determinado por el presidente o el moderador de la sesión.

En esta sesión hay interpretación en inglés, francés, español y árabe. Hagan clic en el icono de interpretación en Zoom y seleccionen el idioma que escucharán durante la sesión. Si desean hacer uso de la palabra, por favor, levanten la mano en la sala de Zoom y cuando el moderador de la sesión diga su nombre habiliten su micrófono. Antes de hacerlo, asegúrense de haber seleccionado el idioma en el que hablarán del menú de interpretación. Digan su nombre para los registros y el idioma en el que hablarán si no es inglés. Al hacerlo, asegúrense de silenciar todos los demás dispositivos y notificaciones.

Hablen con claridad y a un ritmo razonable para permitir una interpretación correcta.

En esta sesión hay transcripción automática en tiempo real. Tengan en cuenta que esta transcripción no es un registro oficial ni autoritativo. Para ver la transcripción en tiempo real hagan clic en el botón de subtítulos en la barra de herramientas de Zoom. Para garantizar la transparencia de la participación en el modelo de múltiples partes interesadas de la ICANN les solicitamos que ingresen a las sesiones de Zoom utilizando su nombre completo. Por ejemplo, nombre de pila y apellido. Podrán ser retirados de la sesión si no lo hacen de esta manera. Gracias y ahora le doy la palabra a Nick Wenban-Smith. Gracias.

NICK WENBAN-SMITH: Gracias por la presentación. Para los que no me conocen, soy Nick Wenban-Smith y yo represento al ccTLD .UK. A los fines de la sesión de esta tarde hasta que la comunidad tenga un mejor presidente estoy dirigiendo el comité permanente de uso indebido del DNS en la ccNSO. Siempre nos interesa tener mucha más participación. Como verán esta tarde, si les interesan estos temas que tratamos, con gusto los recibiremos en nuestro grupo. Tenemos un panel aquí, una representación bastante diversa en nuestro comité permanente pero siempre tenemos lugar para más. Trabajamos de manera colegiada y cooperativa. Nos divertimos y tratamos algunos de los temas tan difíciles que se manejan en la ICANN.

Como verán en la diapositiva, esta tarde vamos a cubrir este temario. Yo voy a tratar de presidir esta reunión y en realidad estoy un poco confundido cuando veo el horario en UTC aquí en la diapositiva pero si no me equivoco esta sesión durará dos horas, aunque eso no lo dice la diapositiva. Con el uso indebido del DNS a veces uno no cree todo lo que ve. Esto es una metáfora.

Vamos a comenzar recordando cuáles son los recursos que estamos proveyendo en el comité permanente del uso indebido del DNS y luego pasaremos al tema central de la sesión donde profundizaremos en distintos aspectos de mediciones y herramientas. Una parte muy importante vinculada con el uso indebido del DNS. Por último, como creo que uno de mis grandes intereses es obviamente asegurar que mi ccTLD sea muy seguro y en segundo lugar que todos los ccTLD sean seguros, valoramos mucho la comunidad y esperamos que entiendan que hay gTLD y ccTLD, y hay muchos puntos en común cuando queremos protegernos del uso indebido. No estamos trabajando en burbujas o en compartimentos estancos cuando hablamos de los ccTLD. Sabemos que el grupo de la GNSO también tiene un grupo dedicado al uso indebido del DNS con los registradores. Nosotros practicamos aquí la cooperación global.

Muy bien. Este es un resumen para quienes están con nosotros por primera vez. La ccNSO no formula políticas para los ccTLD. Tenemos un ámbito de competencia limitado, acotado. Establecemos políticas para determinadas actividades específicas de las funciones de la IANA pero cuando se trata de políticas para los ccTLD en forma individual no tenemos esa función. No estamos aquí para hacer eso.

Como abogado, por supuesto siempre consulto los términos de referencia y todo mi tiempo libre lo dedico a consultar los términos de referencia pero a modo de resumen les quiero decir que esto tiene más que ver con compartir información, conocimientos. Queremos también exhibir aquellos casos de las cosas que funcionan bien cuando se trata de evitar el uso indebido del DNS y también aprendemos de aquellas cosas que no funcionan tan bien. Tratamos de generar concientización, una mayor comprensión. Yo me considero una persona muy abierta y por supuesto admito que cometo errores pero es mucho más útil aprender también de los errores de otras personas y eso también lo hacemos en nuestro comité.

Tenemos un diálogo abierto y constructivo, cuando se da, aunque yo no siento que sea el responsable, creo que se da en un ámbito de colaboración y eso es maravilloso. En última instancia, aunque no desarrollamos políticas queremos darles a todos en la comunidad los recursos que necesitan para ser mejores custodios de sus ccTLD y sobre todo queremos que la Internet sea más segura cuando se vincula con temas del DNS y cuando sabemos que en particular puede haber alguna vulnerabilidad.

Aquí también tenemos el mismo horario. Ven que la pandemia afectó a unos más que a otros. No importa. Vamos a dejarlo así. Como pueden ver, tenemos recursos. Vamos a hablar de herramientas, mediciones y vamos a tener un diálogo. Ahora le voy a dar la palabra a David primero.

DAVID McAULEY: Gracias, Nick. Hola a todos. Soy David McAuley. Soy empleado de Verisign y participo en la ccNSO a través de la administración del dominio de primer nivel con código de país .CC. Participo en este comité permanente sobre uso indebido del DNS. Les doy la bienvenida a mis colegas de la ccNSO y a otros visitantes.

Aquí vamos a recordarles qué es lo que hacemos en un subgrupo que yo dirijo que es el subgrupo del repositorio. Nuestro subgrupo tampoco se ocupa de políticas ni de códigos de conducta sino que se ocupa de crear herramientas de colaboración eficaces para los ccTLD, para la ccNSO y para que los administradores de ccTLD puedan abordar el tema del uso indebido del DNS. Primero vamos a hablar de una iniciativa que es la creación de un repositorio con información útil. Para eso le voy a dar la palabra a Adam Eisner, de CIRA y del ccTLD .CA.

ADAM EISNER: Como dijo David, yo pertenezco al código de país canadiense .CA. Soy Adam Eisner y disfruto mucho del tiempo que le estoy dedicando a esta iniciativa del repositorio. Voy a contarles sobre el repositorio y la biblioteca de recursos que nosotros hemos desarrollado dentro del ámbito del comité DASC.

Teníamos aquí como objetivo crear un espacio dedicado para que los administradores de ccTLD pudieran utilizar como plataforma para compartir información. Aquí tenemos una junta o un comité editorial y asesor de contenidos. Nos reunimos varias veces al mes para revisar las presentaciones de contenido. Los invito a que lo consulten, hagan presentaciones. Esto lo vamos a decir varias veces. Esto es algo nuevo.

Recién está comenzando y queremos tener tanta participación de la comunidad como sea posible como siempre lo hacemos. Esto también se aplica a la información del repositorio.

Nos reunimos un par de veces por mes en este comité editorial para revisar el contenido presentado y también queremos tener algunas reuniones informativas periódicas. Nosotros queremos compartir información y alentar las presentaciones de contenido. Siguiente, por favor.

CLAUDIA RUIZ: Les queremos recordar que hablen lento para los intérpretes.

ADAM EISNER: Tenemos cuatro categorías de contenido en este repositorio. Presentaciones e informes, herramientas que puede usar la comunidad, políticas y definiciones sobre cuestiones vinculadas con el uso indebido del DNS, y luego artículos y comentarios. Cuando visiten el repositorio van a ver esta división en estas categorías. Aquí hay incluido un enlace al repositorio específicamente así que lo pueden visitar cuando quieran.

Los criterios de calificación para lo que se presenta son bastante amplios y como nos vinculamos con ccTLD y con uso indebido del DNS es justamente ese uno de los criterios importantes pero puede haber una amplia variedad de temas del ecosistema, puede corresponder a los registradores, a los registros, temas de amenazas. No importa. Nosotros queremos lanzar una red más amplia en lugar de una

pequeña para tener una gran base de recursos disponibles en este repositorio.

En cuanto al formato, somos bastante flexibles en términos generales. Cualquier formato que utilicen ustedes para consumir información podemos revisarlo. Aquí tenemos un requisito general muy sencillo en ese sentido. Todos los tipos de presentaciones aquí de contenido son más que bienvenidas. Siguiente, por favor.

Muy bien. No es una diapositiva muy buena para que tenga una idea de qué es lo que contiene el repositorio pero aquí tenemos distintos ejemplos para que vean lo que ya contiene el repositorio. Vamos desde entrevistas con el director del instituto de uso indebido del DNS hasta presentaciones que se han hecho dentro de la ccNSO en reuniones anteriores de la ICANN. También hay una amplia gama de definiciones, herramientas y otras cosas. Tenemos aquí una gran variedad de tipos de información que se comunican con distintos públicos sobre distintas cosas y continuamos tratando de generar una base de contenido en estas distintas categorías. Siguiente, por favor.

Por último, en cuanto al proceso, es algo bastante sencillo. No requiere alta tecnología. Estamos recibiendo presentaciones con una dirección de correo específica que ustedes ven aquí en la diapositiva y esperamos recibir toda la mayor información posible. Pueden ver algunos de los datos q idealmente queremos recibir como parte de esa presentación de contenido para que sea más fácil para nosotros categorizar esa información cuando la revisamos y cuando la colocamos en el repositorio. Al cabo de un par de semanas de haber recibido alguna presentación, el grupo en forma individual va a hacer

una revisión y va a llegar a un consenso para ver si lo va a publicar en el repositorio como contenido o no. Como les mencioné aquí un par de veces ya, todas las presentaciones son bienvenidas. Estamos tratando de generar algo nuevo e interesante para la comunidad. Siguiente.

Por supuesto, esto es algo nuevo que se lanzó en la última reunión de la ICANN y está dando sus primeros pasos. Le voy a dar la palabra a David para que cuente sobre otra iniciativa que tiene que ver con la lista de contactos de correo electrónico.

DAVID McAULEY: Como ustedes pueden ver en esta línea cronológica que tenemos aquí en la pantalla, en la ICANN 78 teníamos la intención de anunciar nuestra lista de correos. No cumplimos con la fecha. Estamos creando una herramienta o una lista de correo electrónico que está basada en el modelo descendente. La vamos a pasar al final de esta reunión al DASC. Se va a hacer luego un anuncio a la comunidad sobre esta lista de operaciones de TLD creo que a finales del próximo mes. Siguiente diapositiva.

Dicho sea de paso, dice que Fernando España, de .US, iba a hacer esta presentación. Lamentablemente está enfermo así que con gusto lo voy a remplazar. Siguiente. Tenemos una lista dedicada de correos electrónicos. Les voy a contar los parámetros amplios de esta lista. Como les dije, se va a basar en la lista de operaciones de TLD. Lo que estamos aquí desarrollando es una herramienta de colaboración, correo electrónico, una lista cerrada para administradores de ccTLD. Por supuesto, como es correo electrónico, no podemos garantizar la

confidencialidad porque la gente puede reenviar esos correos. No podemos hacer promesas pero esperamos que sea administrado como TLD Ops, que es algo que en mi opinión ha tenido mucho éxito como herramienta para manejar las cuestiones de seguridad.

En nuestro anuncio el próximo mes vamos a decir que la lista tendrá un elemento para compartir información incorporado. En términos generales habrá indicaciones periódicas de puntos de contacto que serán publicados y esto permitirá también una comunicación fuera de la lista donde alguien pueda ver que ha tenido experiencia con un problema y estará abierta para cuatro suscripciones de cualquier ccTLD. Ese ccTLD va a indicar quién va a estar en ese grupo, va a tener una cuenta con un rol. Pueden tener tres nombres y un rol. Por ejemplo, puede ser el director de política o el director de seguridad. Esperamos aquí que esta lista abarque las áreas de seguridad, los conceptos técnicos, etc. Vamos a tener también resúmenes trimestrales. Es como el repositorio pero aquí se trata de fomentar la colaboración entre los ccTLD para poder afrontar el tema del uso indebido del DNS.

Aquí pueden observar la información que les permitirá saber más sobre esto. Esto es un poquito prematuro porque pondremos esta información en nuestro anuncio. Esta es una buena diapositiva. Por favor, tengan presente esta diapositiva pero tienen que prestar atención a cuando hagamos el anuncio para poder compartirlo con sus colegas de los ccTLD. En el anuncio también vamos a decir que hay información que tienen que darnos para suscribirse a esta lista. Es algo bastante sencillo para suscribirse a la lista. Vamos a tener algunas

notas sobre la naturaleza de esta lista, cómo uno puede acceder a ella. Siguiente.

Este es nuestro equipo del repositorio pequeño con seis personas: Fernando España, Adam, Mary Uduma, Jordi Iparraguirre, Diego Ernesto Luna y yo mismo. Aquí queremos responder a los administradores de los ccTLD y a la comunidad de la ccNSO. Con todas estas herramientas lo que nosotros les pedimos es que las utilicen, como decía Adam. Que nos comenten lo que les parezca de interés, que se suscriban a la lista. Nosotros podemos manejar esto de distintas maneras para lanzarlo de manera adecuada, que responda a sus necesidades. Nosotros vamos a tratar de responder cuando nos pidan que hagamos algún cambio porque queremos que ustedes lo aprovechen. No sé si podemos pasar a la próxima diapositiva.

CLAUDIA RUIZ: Por favor, recuerden hablar lentamente para los intérpretes.

DAVID McAULEY: Le doy la palabra a Nick ahora.

NICK WENBAN-SMITH: Muchas gracias. Es un buen recurso para la comunidad. La siguiente parte de la sesión tiene que ver con indagar en el tema de herramientas y mediciones. Tengo cuatro ponencias diferentes. A nivel personal, todos tratamos de medir las mismas cosas. Por qué están surgiendo diferentes respuestas y qué se supone que haremos con

todos estos mensaje conflictivos en cuanto al uso indebido. Cuando tratamos de hacer algo siempre es el problema de otra persona. Necesitamos diferentes perspectivas.

En la encuesta que nosotros hicimos en el cuarto trimestre de 2022 se hizo una pregunta muy sencilla sobre auto-informes. No siempre tenemos la misma definición de qué significa el uso indebido. Hay diferentes excepciones con respecto a las conclusiones que puedan surgir pero hay dos conclusiones. Una conclusión no nos sorprendió. Tiene que ver con que los ccTLD que participaron en la encuesta tienen cifras muy bajas del uso indebido. Ya sabíamos esto.

Otro punto interesante es lo que se ve en la barra a la derecha. El 38% de quienes respondieron a la encuesta dijeron que no estaban seguros de cuánto uso indebido tenían. Esto hizo que muchos cuestionaran esto el grupo de trabajo. Eso nos preocupó porque si uno es un administrador responsable de ccTLD, se supone que debería saber esta información. De eso se trata esta sesión. De darles a las personas más información con respecto a las herramientas y las mediciones, y la administración de esto.

El uso indebido requiere un grado de sofisticación para detectarlo y por eso la idea es repetir la encuesta, tal vez para el cuarto trimestre de 2024. Sería interesante ver si recibimos las mismas respuestas después de haber tenido este tipo de sesiones para que así las personas afirmativamente sepan el nivel de uso indebido que tienen en vez de estar inseguros.

Ciertos pensamientos introductorios de mi parte para que pensemos de una manera adecuada. El administrar un ccTLD seguro, confiable para su comunidad nacional es uno de los objetivos fundamentales que tiene el operador de registro. Según esta cita, lo investigué, conocía la cita pero no sabía quién había hecho la cita, pero es una buena cita, aunque no se atribuya a la persona adecuada, pero la cita dice: "Si no lo podemos medir, no lo podemos administrar". Por eso yo creo que necesitamos una línea base en cuanto al nivel del uso indebido y después tratar de implementar la política y ver si eso ha tenido efecto. Queremos que esto sea más en base a la evidencia y para administrarlo adecuadamente hay que entender cómo rastrearlo y manejarlo.

Este es mi experimento psicológico favorito, Hawthorne. Ellos han hecho diferentes ejercicios y querían ver si los trabajadores llegan a ser más eficientes según ciertos niveles de luz. Cambiaron las bombillas para saber si los trabajadores serían más eficientes. Una de las cosas que encontraron es que las personas de control, aunque no se les hubiese cambiado la iluminación, aun así todos llegaron a ser más productivos porque se enteran de que se les está observando y eso de por sí cambia el comportamiento de esa persona. Cuando tiene que ver con el medir o rastrear algo, hay una analogía de que cuando uno rastrea o mide las cosas, cambia la conducta. Esto termina mi presentación con respecto a mediciones y ahora entonces le doy la palabra a Rowena.

ROWENA SCHOO: Gracias, Nick. Gracias, DASC y ccNSO, por habernos invitado hoy a hablar de este tema importante. Sigamos a la siguiente diapositiva, por favor. Les voy a dar una introducción breve con respecto a qué es la institución. Después pienso hablar acerca de medir el uso indebido del DNS en general y cómo normalmente se hace y después hablaré un poco más acerca de nuestro proyecto de medición que se llama COMPASS. También hablaré acerca de los retos y después ciertos comentarios finales en cuanto a dónde nos pone esto en el proceso. Gracias.

El Instituto del Uso Indebido del DNS fue creado por el Registro Público de Internet hace tres años. Son una misión sin fines de lucro en los Estados Unidos e invierten el dinero que ganan manejando el registro en algo que sea bueno para el público y para Internet. Cuando hablamos del uso indebido del DNS estamos hablando del uso indebido técnico para nosotros es el phishing, pharming, malware, botnets y spam o fraude, cuando utilicen el mecanismo de entrega.

Estas inquietudes que estaban surgiendo en la comunidad, buscar esas áreas de complejidad, destacarlas y tratar de resolverlas a través de todo el ecosistema. Nos enfocamos no solo el .ORG sino otros TLD y también los registradores. Algo que también es importante es que todo lo que hacemos es libre de costo así que no estoy pidiendo dinero ni estamos vendiendo nada. Estamos más bien proporcionando recursos gratis para que puedan entender mejor el uso indebido del DNS. También tenemos un consejo asesor. Lo forman personas seleccionadas de la comunidad como Bruce y Nick, como sus representantes del ccTLD.

Cuando las personas miden el uso indebido del DNS, normalmente siguen este tipo de proceso. Hay que pensar claramente cuál es el propósito y el enfoque. Muchos estudios con respecto a este tema reciben una información de una lista de bloqueo de reputación y esta lista se crea para el bloqueo de redes más que a nivel de DNS. Hay cientos de estos, sino miles, de una calidad variable. A veces tiene poca evidencia o ninguna evidencia. Ahí es cuando uno tiene que hacer cierta limpieza dependiendo de lo que uno está tratando de lograr.

Como mínimo, si les interesan los dominios únicos, por ejemplo, hay que reducir la lista de URL a una lista de nombres de dominio. A veces para direcciones de IP también se puede incluir en esto, por eso hay que enfocarse en qué quieren medir. Para mí no existe una lista que no tenga algún nivel de falsos positivos, por eso hay que pensar en eso y tomar esto en cuenta a medida que se hace el estudio.

Después, lo que se esté tratando de lograr, hay diferentes niveles de análisis y después decisiones que se tomen en cuanto a la presentación de datos. Hay decisiones difíciles que se deben tomar en toda la lista y esto puede resultar en diferentes resultados y diferentes cifras, hablando de nuevo de la lista de bloqueo de reputación.

Quería hablar un poco acerca de nuestro proyecto, el COMPASS, y las decisiones que hemos tomado durante ese proceso. Cuando nosotros comenzamos el Instituto, necesitábamos tener un entendimiento profundo del uso indebido del DNS para informarle al Instituto de lo que estábamos haciendo pero era también para proporcionarle la información a la comunidad para que ellos se sintieran empoderados en cuanto a lo que está ocurriendo en su zona. Lo teníamos que hacer

a un nivel lo suficientemente granular como para que fuera informativo y que fuera también correcto y compatible a través del tiempo y la industria. Esto tiene que ver con nuestros documentos de mejores prácticas y al final nuestra meta es reducir el abuso del DNS a ese nivel. También tenemos transparencia, credibilidad, independencia, exactitud y fiabilidad.

Logramos esto al colaborar con un investigador independiente y un laboratorio. Maciej Korczynski, quien está aquí sentado en este mismo salón, él es el investigador con el que elegimos trabajar. Es profesor en la Universidad de Grenoble. Trabajamos con el laboratorio KOR y con el Dr. Maciej con respecto a este proyecto de COMPASS.

Es importante hacer notar cuando se fijan en nuestros datos que primero no estamos midiendo todo tipo de daño en el Internet o todas las cosas malas. Más bien estamos optimizando para ver la exactitud y la confiabilidad para asegurarnos de que exista un proyecto completo. También estamos tratando de hacer la comparación a lo largo del tiempo y a través del ecosistema, y también la mitigación fue un paso muy importante para nosotros en este tipo de proyecto cuando comparamos lo comprometido a lo malicioso.

También queríamos entender el tipo de registración. Si el nombre de dominio se registró, si se hizo para el propósito del uso indebido del DNS o si se hizo porque estaba asociado con un nivel de algo comprometido. A veces eso se hace a un nivel de sitio web. A veces esto ocurre cuando están actualizando su sistema de contenido o a veces con el tiempo y así lo explota el actor malicioso. Todo esto hay

que entenderlo para ver qué acción de mitigación hay que hacer y cuál es el riesgo de daños colaterales.

Esto es para darle un visual de lo que yo le estaba explicando con respecto a enfocarnos en ciertos segmentos. De todos los daños que pudieran existir, solo se puede medir lo que se detecta y lo que se reporta. A veces hay personas que lo hablan como un principio iceberg, donde a veces es difícil medir las cosas que no conocemos.

De lo que sí se detecta o se reporta, nos enfocamos en amenazas de seguridad y para este proyecto también tomamos la decisión de enfocarnos específicamente en el phishing y el malware. Tomamos esa decisión porque los colaboradores estuvieron de acuerdo en que esa es una evidencia en la cual confiar. Sé que hay mucha información en esta diapositiva pero ténganme paciencia. Esta es una representación visual de nuestra metodología, que está disponible en nuestro sitio web. Es importante para nosotros que las personas entiendan cómo surgieron estas cifras.

Utilizamos este proceso, como mencioné anteriormente, y este tipo de proceso es algo que unos pocos proyectos comenzaron hace unos años. Uno de ellos es DAAR. Tenemos un conjunto de información que es APWG, PhishTank, OpenPhish, URLHaus. Hacemos un proceso de deduplicación y limpieza. Algo que es muy importante darse cuenta es que alguna de estas listas tiene 70.000 URL con los mismos nombres de dominio. Hay razón para esto. Algunos ataques crean nuevas URL cuando van al nombre de dominio, ya sea humano o de bot. Hay que saber esto. Otro paso importante es que KOR Labs eliminar lo que se entiende por dominios especiales. Estos son dominios donde la acción

a nivel de DNS sería inapropiada. Por ejemplo, proveedores de subdominio, URL cortas, servicios de intercambio de archivos como docs.google.com. Es difícil mantenerlo. KOR Labs los hacen públicamente disponibles hasta el punto de que las personas nos pueden ayudar a actualizar esto. Lo agradeceríamos.

El siguiente paso es un análisis. Hay una huella del sitio, se recogen capturas de pantalla, registros de DNS. Después hay una determinación en cuanto a si el registro es malicioso o comprometido. KOR Labs lo vuelve a verificar para compararlo con las huellas y toda la información que recibieron en el momento que ocurrió. Eso ocurre inicialmente en intervalos cortos de 5, 15, 30 minutos y después una, dos, hasta seis horas y después cada 12 horas durante 30 días.

Finalmente, tomamos esta información y lo resumimos en un reporte público y tomamos decisiones en cuanto a como presentar esa información. Por ejemplo, nuestros informes salen mensualmente. Incluimos tablas con respecto a las tasas de uso indebido del DNS por cada 100.000 DUM. Por ejemplo, si hay niveles bajos de phishing y malware que se identificaron para un mes en particular, entonces los guiamos para evitar los posibles falsos positivos.

Cuando medimos los datos, hay ciertos retos que aparecen básicamente en todos los proyectos. Todas las mediciones son los mejores esfuerzos que se pueden hacer. Hay problemas con falsos positivos. También hablamos de la calidad de la información. También hay áreas grises con respecto a esto. Las simulaciones de phishing a veces parecen reales pero a veces terminan en listas de bloqueos y hay ciertas áreas grises también que es un problema.

Uno de los retos que tenemos en la presentación de los datos es que a veces los datos son sesgados. Muy rara vez es una distribución normal y a veces es difícil cuando tratamos de cifras pequeñas, que es el caso con los ccTLD. También hay ciertos prejuicios geográficos. También tenemos retos con los ccTLD con respecto al tamaño de la zona y registraciones nuevas. Estamos trabajando en ciertas cosas para mejorar ese aspecto también y para que los ccTLD puedan participar.

Este es un breve ejemplo. Puse algo de información aquí y pueden utilizar las otras diapositivas como referencia. En el informe no tomamos un promedio de los últimos 12 meses. Por ejemplo, si hay un nivel alto de uso indebido en más de 100.000, pero solo está allí durante un mes, entonces no publicamos su TLD. Más bien lo redactamos a menos que haya estado allí por cuatro o más. La razón por la que decidí implementar esto es porque si uno es un pequeño TLD como el ejemplo que vemos en la diapositiva, y es el objetivo de un ataque malicioso un mes y mitiga todo, uno todavía puede terminar con un uso indebido muy alto por cada 100.000 DUM. De pronto eso no refleja bien lo que está ocurriendo en ese TLD. La siguiente diapositiva.

¿Qué hace un ccTLD con toda esta información? Piensen cuidadosamente en el propósito que están tratando de lograr, investiguen cuáles son esas cifras y listas y cuáles podrían ser los resultados. Estén al tanto de los falsos positivos. Finalmente ayúdennos a mejorar estos datos. Queremos escuchar de ustedes. Tenemos nuevos tableros de control para cara TLD y para cada registrador. Podemos ayudarles para que ustedes entiendan esas cifras y esta semana hemos lanzado esto a través de un login para que

ustedes se puedan inscribir y verlo en cualquier momento que quieran. Somos buena gente, amigables. Nos gusta hacer esto. Por favor, acudan a nosotros para más detalles.

Este es un breve ejemplo del tablero de control para .ORG. El Registro Público nos dijo que podríamos mostrar esto. Se ven las cifras de malware y al lado derecho se puede ver bajo la administración. La siguiente diapositiva muestra lo que fue comprometido y lo malicioso. Al lado derecho se pueden ver las tasas de mitigación. Creo que eso es todo. Muchas gracias. Estamos disponibles por si tienen alguna pregunta. Pueden ver la grabación si no alcanzaron a ver la presentación o si quieren entrar en detalle. Gracias.

NICK WENBAN-SMITH: Muchas gracias, Rowena. Creo que vamos a dejar las preguntas. Tiene más sentido primero escuchar primero todas las presentaciones y luego tener el espacio de preguntas y respuestas. Me parece que esta es la mejor forma a menos que alguien lo objete. Ahora tenemos a la Federación de Investigación sobre el DNS. Es un placer darle la bienvenida a Nathan Alan.

NATHAN ALAN: Muchas gracias. Es un placer estar aquí. Pasemos a la siguiente diapositiva, por favor. Hoy voy a explicarles quiénes somos en la Federación de Investigación sobre el DNS y el proyecto en el que estamos involucrados con respecto a los ccTLD. Será una descripción general. Podemos usar eso como punto de partida.

La Federación es un organismo sin fines de lucro. Nuestra misión consiste en entender mejor y tener más conocimiento sobre el impacto del sistema de nombres de dominio sobre ciberseguridad, política y estándares técnicos. Lo logramos de distintas formas. Una de las cuales es promoviendo la educación y la investigación sobre el DNS. Nos gusta ayudar a las personas con las que hablamos a acceder a los datos y hemos hecho esto mediante la creación de nuestra propia plataforma de estudios analíticos sobre el DNS a la que me voy a referir hoy. Finalmente participamos en la creación de normas técnicas. Tratamos de ver cuáles son las que se proponen y cómo podemos contribuir en este sentido. La siguiente, por favor.

Este es nuestro sitio web. Aquí vemos algunos de los proyectos de investigación en los que participamos recientemente. El TLD es un proyecto al que me voy a referir brevemente hoy y tiene que ver con los niveles de uso indebido en los distintos tipos de TLD. También tenemos un proyecto de investigación relacionado con normas de Internet o estándares de Internet y la medida de la adopción de RPKI. Finalmente, recientemente comenzamos a trabajar en nombres de dominio de blockchain.

El informe que publicamos a principios de este año era para la unidad constitutiva de negocios de la ICANN quien quería que consideráramos específicamente las tasas de uso indebido de los ccTLD europeos. Queríamos hacer una especie de categorización de todos los ccTLD europeos y también de todos los ccTLD, gTLD y gTLD heredados. Lo abordamos en un nivel muy básico y general. Tomamos una serie de feeds diferentes que teníamos disponibles en nuestra plataforma

analítica y para cada informe que veíamos con respecto a un nombre de dominio en particular lo considerábamos una sola vez, considerábamos ese nombre de dominio una sola vez y eso es importante en esta medición porque lo que queríamos era crear un índice de uso indebido que estuviera basado en la participación de mercado de ese TLD. Lo que queríamos entonces era comparar manzanas con manzanas, por así decirlo.

Un único nombre de dominio actuaba como una única unidad y también veíamos qué pasaba del lado de la registración. Tal como mostraron los datos con respecto a los ccTLD, los ccTLD tienen niveles más bajos de uso indebido. Los ccTLD europeos tuvieron los niveles de uso indebido más bajo. Entonces el informe que nos pidieron que preparáramos tenía que ver con entender cuáles eran los TLD que tenían el menor índice de uso indebido y ver qué hacían para generar esos niveles de uso indebido tan bajo en comparación con otros. La siguiente, por favor.

Este es nuestro sitio web. Una vez más, pueden visitarlo, ver la parte de investigación para acceder a los datos que presentamos. También aquí en la ICANN tenemos un stand. Si quieren tener información más detallada acerca de cómo preparamos y cómo llegamos a los índices y a las conclusiones a las que llegamos con todo gusto podemos compartir esa información con ustedes también.

El índice, y eso es especialmente para los ccTLD europeos, porque el informe que presentamos estaba basado en esto, obviamente había niveles bajos de uso indebido y vimos que en realidad no había una única solución, no es que todos los que tenían niveles bajos de uso

indebido hacían lo mismo. Todos actuaban de forma proactiva, tenían abordajes proactivos y el estudio no solamente tomó en cuenta el uso indebido que vimos en los datos que habíamos recopilado sino que también tomaron datos de CENTR, un estudio de CENTR que nos sirvió para entender cuáles eran algunas de las medidas que tomaron estos registros en cuanto a entender sus clientes, conocerlos, hacer análisis de los registratarios, revisar los datos y asegurarse de que los datos fueran precisos y correctos. Como dije, había diversas medidas que se tomaron. No es que hubiera una única medida exitosa. La siguiente, por favor.

Esta diapositiva muestra una vez más dónde pueden encontrar vínculos para acceder a este informe y creo que esta es la última diapositiva. No. Este es un análisis detallado de la tabla que preparamos y separamos la cantidad de informes que vimos en la plataforma que estaba relacionada solamente con el nombre de dominio, el nombre del host, a diferencia del URL. Aquí desglosamos estos números pero, como dije, tenemos aquí un puesto, un stand en la ICANN así que si quieren más información, acérquense. Podemos incluso darles una demostración del sitio. Estos son los vínculos para poder acceder a los diversos recursos que yo mencioné. Eso es todo, creo. Gracias.

NICK WENBAN-SMITH: Muchas gracias, Nathan. Ya tenemos dos, tres creo yo, recursos a los que pueden acceder todos los que están aquí para medir los índices de uso indebido. Las metodologías son levemente diferentes. Ahora le doy la palabra a Samaneh. Prefiero llamarla solamente Samaneh, no

sé por qué. Samaneh va a hablar acerca del trabajo que hace en la organización de la ICANN en cuanto a medir los niveles de uso indebido. Una vez más, lo vamos a ver desde una lente levemente diferente.

SAMANEH TAJALIZADEHKHOOB: Gracias, Nick. Soy Samaneh. Pertenezco al equipo de seguridad, flexibilidad y estabilidad de la ICANN. Esta presentación la preparé junto con mi colega, el Dr. Sion Lloyd. Hicimos esta presentación que es un poco distinta de las presentaciones típicas de la ICANN. Comenzamos con la pregunta: ¿Qué es lo que están tratando de hacer los investigadores en la comunidad en materia de uso indebido del DNS? La mayoría de las presentaciones y del trabajo de los investigadores muestran que la gente está tratando de identificar el uso indebido mediante algunas métricas.

Lo que queríamos ver era por qué eran importantes estas métricas o indicadores, y por qué siempre estamos tratando de crear mejores indicadores para tener más exactitud y confiabilidad. Aquí pueden ver los mismos datos presentados de dos formas diferentes. El gráfico que está a la izquierda muestra el recuento crudo de uso indebido. A la derecha vemos los porcentajes. Cada punto representa a un TLD.

Lo que observamos es que podemos llegar a tener un panorama muy diferente si consideramos los datos utilizando diferentes indicadores. Podemos obtener los mismos datos presentados de dos formas diferentes y llegar a conclusiones diferentes mirando el mismo subconjunto de datos. Por eso es tan importante prestar atención a la

forma en que creamos indicadores y cómo informamos acerca de estos indicadores.

Qué puede servir para que las métricas o los indicadores sean mejores. Datos de más calidad, con menos falsos positivos, tal como dijo ya Rowena. Cuando se trata de determinadas clases de conjuntos de datos, por ejemplo, los datos de las listas de bloqueo de reputación, casi no hay datos sin falsos positivos. Podría haber indicadores para mejorar la calidad de la totalización de los datos y para limpiar los datos.

También podríamos tener definiciones más precisas de lo que se mide. Por ejemplo, con frecuencia escuchamos hablar acerca de spam como correo no solicitado a diferencia del spam como mecanismo de entrega de malware. Esto es una diferencia muy importante para nuestra comunidad.

El tercer punto es incorporar errores de medición, reconocer que los datos de los que estamos hablando, es decir, si estamos hablando de una lista en particular, porque RBL, la lista de bloqueo de reputación, tenemos que saber qué nos puede dar esa lista y qué no nos puede dar. Si mostramos un gráfico, vemos que un gráfico nos muestra una cosa pero otro gráfico nos muestra lo mismo de forma diferente. Tenemos que entender por qué. La siguiente, por favor.

¿Quiénes somos dentro de la ICANN? La siguiente diapositiva, por favor. Nosotros somos el grupo de investigación sobre seguridad, estabilidad y flexibilidad de la ICANN y trabajamos en torno a los identificadores de seguridad de Internet. El objetivo de nuestro grupo

es aumentar la confiabilidad de los indicadores que miden la seguridad relacionada con los identificadores. ¿Comenzamos a partir de indicadores que ya existen y los mejoramos o desarrollamos nuevos indicadores desde cero?

El uso indebido del DNS es un tema en el que trabajamos. También trabajamos con otros indicadores relacionados con la seguridad. El núcleo de nuestro trabajo consiste en utilizar datos y métodos científicos para responder a las preguntas que le interesa responder a la comunidad. La siguiente diapositiva, por favor.

Este es un esquema de trabajo general de nuestro grupo. Tenemos que tener en cuenta que el objetivo principal de la creación de mejores indicadores es poder medir la seguridad relacionada con los identificadores. Nosotros recabamos datos y creamos indicadores o métricas. Este es un ejemplo de alguno de los proyectos en los que trabajamos. Los datos que recabamos con frecuencia son datos que representan la situación de un dominio. Por ejemplo, archivos de zona que contienen información acerca del espacio de nombres de dominio. También podrían ser los datos de enrutamiento en el caso de las direcciones IP o datos de una lista de bloqueo de reputación.

Tomamos mediciones para que todos estos conjuntos de datos sean una mejor versión. Por ejemplo, cuando hablamos de los datos de las listas de bloqueo de reputación tenemos un proyecto que se centra en crear métodos para evaluar la lista de RBL que utilizamos nosotros, que utilizan los miembros de la comunidad y también los miembros del panel al igual que la comunidad científica, sea quien fuere que utiliza estas listas.

En materia de archivos de zona, lo que hacemos es desarrollar métodos para básicamente representar las partes de la zona del espacio de nombres de dominio que están activas en comparación con aquellas que no están activas. Por ejemplo, dominios estacionados. En el trabajo que publicamos este año surgió que casi un 20% de las zonas no están activas.

Luego tenemos también proyectos en torno a datos informados. Por ejemplo, correo electrónico no solicitado. El grupo de trabajo antiphishing, que es diferente de los feeds del grupo antiphishing que se usa en la comunidad, trabajamos con clasificadores para clasificar los tipos de amenazas y mejorar los indicadores en relación con esto y cuando se trata de medir el uso indebido tenemos el proyecto DAAR que es la herramienta de informe de actividad de uso indebido que seguramente ustedes conocerán. Tenemos proyectos para medir el tiempo de actividad de los dominios registrados de forma maliciosa y esto está en un informe sobre las listas de bloqueo de reputación. Esto es en pocas palabras aquello en lo que se centra nuestro grupo de trabajo.

Ahora voy a dedicar un par de diapositivas a hablar acerca de las herramientas DAAR porque sabemos que algunos ccTLD están participando en este proyecto y por lo tanto quisiéramos escuchar sus opiniones y también hablar acerca de los avances de este proyecto sobre el informe de actividades de uso indebido de dominios.

La mayoría de ustedes sabrán que este proyecto totaliza datos de RBL a nivel de TLD y lo combina con la cantidad de dominios del archivo de zona similar a lo que mencionaron ya mis otros colegas. El proyecto

está operativo desde 2017. Produce informes mensuales. En general estos informes mensuales se publican para los TLD y los TLD tienen acceso también a sus propios números de uso indebido a través de la API de la ICANN. Dado que esto existe desde hace bastante tiempo, también nos permite crear tendencias de largo plazo y análisis. La siguiente, por favor.

Estos son los ccTLD que se ofrecieron como voluntarios para participar en este proyecto. Una vez más, les agradecemos a los ccTLD por haber participado y por todos los aportes que recibimos de ellos. En materia de los ccTLD, además de los datos estadísticos que reciben de la API de ICANN también reciben un informe mensual individualizado personalizado para los ccTLD. La siguiente, por favor.

Este es un ejemplo de la clase de datos que figura en los informes mensuales. A los fines de esta presentación yo quité los nombres y en el gráfico aparece .CC, que es un ejemplo de un ccTLD. Lo utilizamos como muestra, como ejemplo. No representa a ninguno de los ccTLD que participaron en el proyecto.

Los gráficos que ustedes ven en pantalla muestran la distribución de los cuatro tipos de amenazas que utilizamos en el proyecto DAAR en el espacio de ccTLD y gTLD. Como pueden ver, parecería que el spam como mecanismo deliberado es lo que más se utiliza pero se concentra más en el espacio de gTLD que en el espacio de ccTLD al igual que ocurre con otro tipo de amenazas.

Este es un ejemplo de los gráficos que figuran en el informe personalizado para ccTLD que les enviamos a todos los cc y a todos los

contactos técnicos de los códigos de país que tenemos. Si se fijan en el gráfico verán que hay un punto azul, punto cc. Esos puntos permiten que los participantes se identifiquen a sí mismos y se puedan comparar con el resto del espacio. Este gráfico en particular muestra dónde está cada TLD en general, cuál es su desempeño en términos de porcentaje de uso indebido por tipo de amenaza: phishing, malware, spam como mecanismo deliberado, y botnet comando y control. El tamaño del círculo indica el grado de uso indebido que se informa en las listas de bloqueo de reputación. La siguiente, por favor.

Una vez más, este es otro ejemplo de los gráficos que figuran en los informes para los ccTLD, los que reciben los administradores de ccTLD, y permite que cada ccTLD se pueda comparar con sus pares y aquí vemos las tendencias a lo largo del tiempo y el uso indebido desde octubre de 2022 hasta la fecha.

Como pueden ver, hay diferencias en cuanto a la concentración y a la evolución de la concentración de uso indebido en los ccTLD. Quiero decir y aclarar que la precisión y confiabilidad de nuestros datos se basa en el indicador más básico que tenemos que es la cantidad de puntos de datos que tenemos. En el caso del espacio de los gTLD, la cantidad de puntos de datos es la cantidad de gTLD que tenemos en los datos y es mucho mayor que lo que tenemos en el caso de los ccTLD porque los datos de ccTLD son limitados. Están limitados a la participación de aquellos que se ofrecen como voluntarios para participar. Cuantos más voluntarios haya, mayor será la precisión de los datos estadísticos y los gráficos que creamos. La siguiente, por favor.

Esto es lo que el proyecto puede y no puede hacer. El proyecto tal como está en su estado actual no puede informar acerca de ningún otro nivel que no sea TLD. No tenemos indicadores sobre registradores o nombres de dominio. También podemos crear un análisis histórico de las amenazas de seguridad y ayudar a los operadores a entender dónde están en comparación con el resto de sus pares en el espacio. Como los datos están anonimizados y totalizados, no se refieren a un dominio en particular que figure aquí. No tenemos una jerarquía pública de registros por el momento.

¿Por qué a los ccTLD les debería interesar participar en DAAR, dado que es para los ccTLD y tenemos ccTLD que participan muy activamente? En primer lugar y lo más importante, los informes que les enviamos a los ccTLD les permitirán compararse con sus pares. Podrán ver dónde están, cómo se comparan, aunque cuando no tengan los números específicos, sí podrán entender cómo le va a cada uno en comparación con el resto. Esto nos ayudará a nosotros también a darles mejores indicadores. Si tenemos más ccTLD tendremos indicadores más precisos. Al participar en el programa ustedes nos podrán dar información. Podremos modificar el informe con los aportes de todos ustedes y de esta forma podremos influir incluso sobre la visualización, la metodología, y las herramientas que usamos serán mejores y por tanto ustedes recibirán mejores resultados. También ustedes podrán utilizar los indicadores que nosotros creamos para el monitoreo interno como ccTLD. La siguiente, por favor.

¿Cuáles son los próximos pasos? El equipo DAAR está trabajando y será liderado por Sion Lloyd, un colega,

para desarrollar la próxima versión del proyecto. La próxima versión, ya hace un año que estamos trabajando para definir los requerimientos y las especificaciones del proyecto. En las próximas dos diapositivas voy a referirme a cómo va a evolucionar este proyecto. La siguiente, por favor.

En primer lugar, en la próxima versión… Perdón. ¿Podemos pasar a la siguiente diapositiva? Me parece que hay un error aquí en la presentación. No importa. En la próxima versión vamos a tener una plataforma de medición que será modular. Eso significa que cada tanto vamos a dar a conocer un módulo con determinada funcionalidad. El primer módulo va a incluir lo que tiene el DAAR actualmente más los indicadores de los registradores. En el próximo módulo que se anunciará de aquí a nueve meses o un año se incluirán indicadores para los registros y los registradores. Habrá un tablero de control dinámico que permitirá que los usuarios vean los datos de nivel de dominio y también datos a nivel de registro y registrador para las búsquedas. También habrá una API conectada para que los investigadores puedan obtener los datos si lo necesitan para usos en la comunidad académica, si quieren utilizar otros canales además del tablero de control de la web.

Lo que ven en esta diapositiva son planes a más largo plazo para este proyecto. Por supuesto, quisiéramos tener participación de más ccTLD, escuchar qué es lo que consideran que les podría ser útil. En el futuro, no en el módulo uno sino en los futuros módulos pensamos tener también el tiempo de actividad medido, tener un indicador, la cantidad de tiempo durante la cual un dominio está desde el momento

de la registración activo para esa actividad maliciosa. También queremos distinguir entre los dominios registrados con fines maliciosos y los comprometidos. Esta herramienta también nos puede dar puntajes de riesgo para tener medidas predictivas.

Estos son los planes a futuro. Les digo nuevamente a los ccTLD a los que les pueda interesar o que tengan preguntas que se acerquen, que nos hagan sus comentarios si les interesa participar. Tengo una diapositiva que está oculta aquí pero que tiene todos los pasos que indican cómo un ccTLD se puede sumar a este proyecto DAAR. Siempre se pueden acercar y hablar conmigo, por supuesto.

NICK WENBAN-SMITH: Gracias, Samaneh. Aquí teníamos un tema encarado desde una perspectiva levemente diferente pero nuevamente los ccTLD tienen que decidir ser incluidos en el DAAR. Esperemos ver si se suman más ccTLD y esto es otro ejemplo de que hay otra manera más de hacer un recorte de los datos a partir de distintas fuentes. Yo tengo algunas preguntas pero vamos a pasar a la última presentación sobre esta sesión de indicadores. Aquí tendremos un levemente diferente pero también sumamente interesante desde el punto de vista de los ccTLD. Vamos a hablar de la colaboración de los registros del operador del registro .NL y el belga, .BE. Vamos a darle la palabra a Thijs Van den Hout.

THIJS VAN DEN HOUT: No sé si tengo que esperar a que proyecten las diapositivas. Supongo que no. Me voy a presentar. Soy Thijs Van den Hout. Soy investigador en SIDN Labs. Estoy aquí con Ronald Geens, quien es director de relaciones externas en .BE, de Bélgica. Trabajamos en forma conjunta para detectar registraciones con fines maliciosos.

En esta presentación vamos a hablar de algunas cosas. Primero les voy a introducir RegCheck, que es el nombre del proyecto en el que estamos colaborando. Es una aplicación con base en el aprendizaje automático que detecta registraciones con fines maliciosos. SIDN utiliza RegCheck en su abordaje desde el momento de la registración hasta el último paso. Les voy a explicar cómo nosotros usamos RegCheck.

Luego Ronald va a hablar de cómo ellos manejan las registraciones maliciosas en .BE y qué es lo que piensan hacer para el futuro. Vamos a hablar un poquito en mayor detalle de la colaboración entre los registros y luego compartiremos las lecciones aprendidas hasta el momento. Ya podemos pasar a la siguiente diapositiva.

Esto es RegCheck. Como dije antes, es una aplicación basada en el aprendizaje automático para detectar registraciones con fines maliciosos en el momento de la registración. Esta presentación la di hace unos días así que tal vez haya alguna superposición si estuvieron en esa sesión. Si necesitan más detalles pueden recurrir a la presentación que hice en ese momento.

A modo de esquema aquí ustedes pueden ver que RegCheck tiene algunos componentes técnicos. El primero es un conector de

registraciones que conecta las registraciones de un registro con la aplicación RegCheck. Tenemos una base de datos RegCheck que contiene información sobre registraciones pasadas y etiquetas que se utilizan para entrenar el módulo de aprendizaje automático. Luego tenemos también un componente con un bloque de aprendizaje automático RegCheck ML con componentes plug and play, con distintos métodos de detección que se pueden utilizar o distintas funciones que se pueden tener en cuenta, características que se pueden ver en las registraciones de los nombres de dominio para tratar de averiguar si se registra de manera maliciosa o no.

RegCheck va a hacer una prueba de la registración del nombre de dominio y va a dar un puntaje de riesgo como resultado. La escala será de 1 a 100 y ese puntaje determinará cuánta probabilidad hay de que esa registración se torne maliciosa en el futuro. El registro puede utilizar RegCheck ofreciendo un par de ingredientes. Primero registraciones obviamente, registraciones pasadas en combinación con información de fuentes, de etiquetas o de uso indebido. Se utilizan para entrenar el módulo de aprendizaje automático, para que detecte estas registraciones. Luego se pueden hacer pruebas de las nuevas registraciones en RegCheck y se le puede asignar el puntaje.

El registro va a necesitar analistas de uso indebido para interpretar ese puntaje o para determinar la política con la que van a abordar estas cuestiones. Luego conocimiento de aprendizaje automático para poder completar esos bloques de aprendizaje automático que mencioné. Se puede personalizar según los requisitos de los registros. Puede tener en cuenta determinadas características o rasgos según

ese puntaje. Los registros tienen que tener una idea de qué características quieren incluir. Luego, cuando RegCheck asigna un puntaje de riesgo a una nueva registración de nombre de dominio y se excede un valor de umbral, el registro va a tener que tener una política y una implementación técnica para determinar cómo manejar esa registración. Puede haber muchas diferencias entre los registros en este sentido como voy a ilustrarles en las próximas diapositivas. Siguiente, por favor. Aquí hay un clicker. A ver si funciona. Muy bien. Ahí está.

El abordaje que utilizamos en el SIDN para .NL es algo que venimos aplicando desde hace un tiempo ya. Vamos a comenzar con lo primero. Todas las nuevas registraciones ingresan al archivo de zona. No hacemos delegación diferida, incluso cuando sean nombres de dominio riesgosos. Hacemos un cálculo de los puntajes de riesgo en retrospectiva con RegCheck.

Tenemos una nueva registración que ingresa a la aplicación de RegCheck. El clasificador de RegCheck va a analizar esa registración. Le asignará un puntaje de riesgo. El clasificador es un gran filtro donde los datos de entrada son todas las registraciones y el producto son solamente aquellos que superan un umbral para ese puntaje de riesgo. Publicamos esas registraciones de alto riesgo en un tablero de control para tener un segundo filtro. Aquí hay una intervención humana que verifica los resultados de RegCheck y si también consideran que son registraciones con fines maliciosos o si hay algo extraño, inician una respuesta en forma de una verificación de identidad. Le envían una consulta al registratario para que verifique su identidad. Si no lo hacen

al cabo de tres días se puede sacar de línea ese dominio. El beneficio de este abordaje es que somos muy exactos y muy diligentes en nuestra respuesta. La desventaja es que requiere mucho trabajo manual, tenemos colegas que dan soporte analizando los resultados y todavía tenemos un tiempo de respuesta bastante largo de tres días. Ahora le doy la palabra a Ron.

RONALD GEENS: Hay una segunda diapositiva.

THIJS VAN DEN HOUT: Conoces mejor mis diapositivas que yo. Este es un ejemplo del tablero de control. La registración pasa o no pasa. Esa verificación de RegCheck queda informada en este tablero por el tipo de sistema que usamos de aprendizaje automático. Se asigna este puntaje y vemos qué características de la registración del nombre de dominio son las que más contribuyen a este puntaje de riesgo. En este caso del juego, tenemos algunos caracteres en el nombre de dominio y también una dirección que es inválida. En total vemos que el 44% de las verificaciones de identidad solicitadas se inician por este paso de verificación de RegCheck. Gran parte del trabajo del equipo de soporte comienza por RegCheck y menos del 5% de los registratarios responden a estas solicitudes de verificación de identidad, lo cual puede indicar que tenemos que pode hacer saber cuáles podrían ser maliciosas en el futuro.

La evaluación cuantitativa es bastante difícil. Solamente podemos asignar números a una evaluación. Compararlos con informes o denuncias de uso indebido. A medida que vayamos mejorando RegCheck tendremos menos informes de uso indebido que usar como base para la evaluación. RegCheck podría funcionar 100% correctamente. No habría puntajes de riesgo. Todo sería 0 y no necesitaríamos ningún indicador. Si alguien tiene una idea de cómo evaluar un sistema como este desde el punto de vista cuantitativo, con gusto escucharemos sus ideas. Este es el abordaje de .NL. No hay una verificación diferida. Se comienza con la registración y luego se pasa a la verificación de identidad para aquellos que son considerados de alto riesgo.

RONALD GEENS: Ahora continúo yo con la próxima diapositiva. En DNS Bélgica tenemos la delegación diferida del proyecto de delegación del 2020. Primero no usábamos ningún abordaje con aprendizaje automático. Usábamos un sistema en base a reglas que podía utilizarse. Las reglas se evalúan de manera continua y se adaptan a lo que necesitamos.

El sistema funciona de la siguiente manera. Un registratario quiere registrar un dominio a través de un registrador y la combinación del nombre de dominio y del identificador de contacto se utiliza para un abordaje en base al riesgo. El sistema de riesgo, se supone que si no es de alto riesgo entramos el dominio en el archivo de zona. Si no ingresa allí, el registratario recibe una invitación para verificar de manera automática su identidad y, solamente cuando lo haya hecho, ese nombre de dominio puede ingresarse al archivo de zona.

Como les dije, este es un sistema basado en reglas que utilizamos actualmente. Estuvimos experimentando con un sistema basado en aprendizaje automático in situ en paralelo y lo que hemos visto es que este sistema ha estado creciendo durante un periodo bastante extenso y de hecho se volvió demasiado complejo. Nos pusimos en contacto con SIDN y trabajamos juntos ahora para empezar a utilizar el mecanismo de RegCheck para remplazar nuestro sistema basado en reglas para este abordaje para la delegación diferida.

La gran diferencia aquí es que nosotros no hacemos delegaciones si consideramos que el riesgo es demasiado alto. Esto es una diferencia importante pero también utilizamos el aprendizaje automático de manera diferente porque si bien a fin de cuentas el objetivo es optimizarlo al mayor nivel de precisión posible para evitar tener falsos positivos, diferimos los falsos positivos en lugar de tener algo más exacto. Esto significa que necesitamos otro control, otra verificación adicional pero nos aseguramos de poder detectar mayor cantidad de situaciones de uso indebido.

Otra diferencia que hemos observado es que se utilizan datos de entrada para entrenar el sistema. También tenemos una lista de uso indebido que usamos para entrenar el sistema. Además, también tenemos en cuenta los casos en los que el registratario verifica los datos de WHOIS. Esto nos da datos adicionales que esperamos que podamos usar para tener una revisión más exacta y lo que más que nada queremos detener es el phishing en nuestro caso. Eso es todo de mi parte.

THIJS VAN DEN HOUT: Siguiente diapositiva. Podemos resumir nuestro avance en estas tres fases de colaboración. Como dijo Ron, ambos registros comenzaron a experimentar con el aprendizaje automático para tratar de detectar las registraciones con fines maliciosos. En marzo del año pasado, en SIDN presentamos en una reunión de investigación y desarrollo un prototipo y un estudio de factibilidad para RegCheck y DNS Bélgica se dio cuenta de que había un terreno en común, entramos en contacto, empezamos a intercambiar ideas, distintos enfoques que habían asumido los registros para abordar este problema y al final de esa fase de exploración llegamos a la conclusión de que RegCheck era una buena base para un proyecto conjunto, más maduro y fácilmente adaptable.

En diciembre de ese año firmamos un acuerdo de colaboración y allí decidimos compartir la propiedad de la base de datos de RegCheck y la propiedad intelectual y desde entonces seguimos trabajando en el desarrollo conjunto de RegCheck fusionando las bases de DNS Bélgica y SIDN para tener una mejor versión de RegCheck. Siguiente, por favor.

En los últimos seis meses venimos colaborando estrechamente, trabajando con una base de códigos única y nos dimos cuenta de que colaborar en un proyecto como este aporta muchos beneficios más que hacerlo en forma individual. Voy a compartir algunos de ellos aunque son un poco técnicos.

Más que nada una de las cosas que un registro consideró antes y luego el otro no, y ahora lo consideran en esta base conjunta es que mejora la puntuación de reputación. Nosotros calculamos la reputación en un periodo y esto nos da un puntaje de riesgo que lo mitigamos mejorando el algoritmo que utilizamos para ello. También

introdujimos la validación de rasgos geográficos, la ciudad y el huso horario por ejemplo del registratario. Hemos mejorado la manera de codificar la relevancia de algunos campos con un abordaje para recuperar la información TF-IDF como la ciudad o el país del registratario. También cambiamos la manera en que vemos el nombre de dominio como factor de riesgo, solamente teniendo en cuenta aquellas combinaciones de caracteres que también se producen un par de veces en las registraciones maliciosas. A nivel más general o más estratégico hablamos sobre el diseño de la aplicación y las selecciones de tecnología que podemos hacer para tener una herramienta con base en un código más genérico y de mejor calidad. Siguiente diapositiva.

Ahora, para ir cerrando, algunas lecciones que aprendimos en el último año. Aprendimos que, en primer lugar, compartir experiencias con otros y también opiniones diferentes sobre el uso indebido es sumamente valioso. Estuvimos mostrando en la fase exploratoria qué hicimos los dos registros para abordar las registraciones maliciosas, el uso indebido y qué es lo que hicimos de manera proactiva juntos. Esto ha sido muy valioso. Vimos que la colaboración funciona muy bien incluso cuando hay políticas divergentes. Como ustedes escucharon, los dos abordajes son bastante diferentes en .NL y .BE pero igualmente pudimos avanzar en el desarrollo de una única aplicación que se puede utilizar en ambos escenarios. No hay que estar de acuerdo en todo necesariamente para poder colaborar.

También aprendimos que la colaboración inspira a la innovación, ya sea a nivel técnico, aprendimos nuevos componentes técnicos,

paquetes de software que no utilizábamos, pero también a nivel de política aprendimos. Por supuesto, más personas implica más opiniones. Aunque tenemos un tiempo de corrido un poco más extenso, tenemos distintas opiniones sobre las decisiones tecnológicas y de diseño y esto es algo que podemos superar. Eso es todo de nuestra parte. Gracias.

NICK WENBAN-SMITH: Muy bien. Gracias. Este es un ejemplo de la colaboración con ccTLD y el trabajar eficazmente para poder reducir el uso indebido, eso espero. ¿No hemos leído si el RegCheck impide el uso indebido o no, o si estamos en una etapa demasiado temprana como para detectar eso?

THIJS VAN DEN HOUT: Es difícil crear un modelo en base a solo informes pero en este caso diríamos que sí, definitivamente.

NICK WENBAN-SMITH: Tenemos un equipo de liderazgo en el lado oscuro, no, es un chiste, tenemos aquí a Brian y Alan, del grupo de partes interesadas de registros de la GNSO, que se van a unir a nuestra sesión. Podría ser malo y decir que más bien se mantengan en ese lado, con todas las personas malas de allá. Sea como sea que se fijen en los ccTLD, tienen estadísticas más bajas de uso indebido. El proceso de registración si nos fijamos en la fricción, en cómo los holandeses y belgas detectan algo de alto riesgo antes de que ocurra. Es muy eficaz. No sé si eso es

una correlación o una causa. Por eso quería compartir eso con ustedes. Voy a darle la palabra a Joke para que lea algo del Zoom.

JOKE BRAEKEN: La primera pregunta es de John McCormack. ¿Hay un enlace para el paper que tenía un estacionamiento aproximado del 20% en TLD?

SAMANEH TAJALIZADEHKHOOB: Sí. Se publicó ese documento y lo puedo proporcionar a nuestro colega de la ccNSO.

JOKE BRAEKEN: ¿Puede explicar por qué se lista aquí el estacionamiento de dominios? ¿Lo considera como algún tipo de uso indebido?

SAMANEH TAJALIZADEHKHOOB: Hablé de esto en esta sesión en particular porque cuando hablamos del espacio de dominio incluidos en los archivos de zona, consideramos que todos los dominios son dominios activos al igual que los dominios que están en la lista de bloqueo de reputación. Ahora, si miran las listas a diario y ven si están activos o no, uno saca una conclusión diferente y una de las categorías donde los dominios pueden ser inactivos es porque puede ser que sea debido a las categorías según nuestra investigación y que se publicó.

NICK WENBAN-SMITH: ¿Alguna pregunta en la sala? Lo puede leer en vivo o grabarlo.

CHRIS DISSPAIN: Estaba tratando de alzar la mano virtual. Chris Disspain, del consejo de la ccNSO. Quiero aclarar algo. Creo que Nathan, de pronto le escuché mal, pero creo que en su diapositiva habló acerca del uso indebido del DNS pero después habló del uso indebido de Internet. Quiero saber si es que estamos hablando de un tema más amplio o es que quiso decir usted uso indebido del DNS. Segundo, noté de dónde saca los datos. ¿Tiene una definición de lo que cree usted que es el uso indebido del DNS, si es la misma definición que utiliza COMPASS?

NATHAN ALAN: Las fuentes que utilizamos de los usos indebidos que medimos son de OpenPhish, APWG e incluimos datos de SpamHaus en este estudio. Yo diría que los datos disponibles están en el sitio web y esperamos mejorar eso para que entonces puedan filtrar ciertos tipos de uso indebido si es lo que quieren hacer pero sí, creo que la forma en como definimos el uso indebido es muy similar. Simplemente fue en base a eso que hablamos del uso indebido del DNS.

NICK WENBAN-SMITH: Una pregunta más.

ANDREA GLANDON: Bart tiene la mano alzada.

BART BOSWINKEL: Gracias, Andrea. Hubo una pregunta de Luc Seufer con respecto a RegCheck. Él quería saber si de pronto se mencionó el porcentaje de falsos positivos de RegCheck. Queremos saber eso.

THIJS VAN DEN HOUT: Los falsos positivos han fluctuado un poco. Depende de lo que usted llame falso positivo. Si estamos hablando de informes falsos de uso indebido tenemos una precisión del 20% pero es difícil evaluar eso porque RegCheck a veces encuentra cosas que Netcraft encuentra o no encuentra, y Netcraft encuentra cosas que RegCheck no encuentra, así que es complementario uno con el otro. Por eso es difícil descifrar cuántos falsos positivos realmente son falsos positivos o si simplemente están encontrando cosas que no encontró Netcraft. En general, con respecto al puerto de datos de uso indebido, yo creo que 25-50% se le hace seguimiento a lo que se pone allí. No sé actualmente cuáles son las cifras. Lo dejaré aquí.

NICK WENBAN-SMITH: Hay otra mano.

JUTTA CROLL: Gracias. En base a estas presentaciones y a otras sesiones previas del GAC entiendo la definición del uso indebido del nombre de dominio y lo que dice ICANN pero me pregunto si el esparcir malware eso se considera uso indebido del DNS o cuando distribuyen material de

abuso infantil, si eso se incluye en eso o no. No sé si eso es debatible o de pronto no es un tema para un debate en ICANN. Gracias.

NICK WENBAN-SMITH: ¿Alguien quiere contestar eso?

BRIAN CIMBOLIC: Quiero corregir que Alan y yo somos del grupo de partes interesadas de registros, no de la GNSO. Es una buena pregunta. Creo que cuando estamos hablando acerca de uso indebido del DNS hay personas que piensan que simplemente porque no es uso indebido del DNS no es terrible. Creen eso, que no se debe solucionar esto en línea, pero cuando los registradores hablan del uso indebido del DNS, se está hablando de usos indebidos manejados apropiadamente a nivel de DNS y material con respecto a abuso infantil. Es terrible. Identity Digital, Nominet, todos tenemos programas robustos para lidiar con estos materiales de abuso infantil pero porque tomamos acción en ello, eso no quiere decir que sea uso indebido del DNS. Sé que suena confuso pero si piensan en esto, el 99% de materiales con respecto a abuso infantil están en sitios que comparten archivos. Eso quiere decir que puede existir un porcentaje del porcentaje del porcentaje, o sea, 0.0001% del contenido del sitio web que tenga que ver con materiales de abuso infantil pero a nivel de dominio lo único que podemos hacer es analizar todo el nombre de dominio. Tal vez el contenido no tenga nada que ver con el material de abuso infantil. Como tenemos una herramienta limitada para lidiar con esto, tenemos que ser muy cuidadosos cuando estamos hablando del tema de qué es apropiado

en cuanto al uso indebido del DNS. Con esto no estoy diciendo que no sea terrible. Simplemente no somos los actores apropiados debido al daño colateral que pueda ocurrir cuando tomamos acción en ello.

JUTTA CROLL: Tenemos datos de nuestros clientes. Esperamos que se esté haciendo el traslado desde los servidores de intercambio de archivos hacia el dominio. Creo que es buena idea fijarnos en ese tema. Gracias.

ORADOR DESCONOCIDO: Nick, Alan Woods tiene la mano alzada.

ALAN WOODS: Estamos hablando de lo que dijo Chris Disspain. Yo no tengo nada más que añadir en ese aspecto pero en cuanto a la pregunta de Chris Disspain, bueno, tal vez no era de Chris, pero tiene que ver con una pregunta de recursos. Una de las perspectivas de las que yo puedo hablar en base a nuestra experiencia del grupo de múltiples partes interesadas y el grupo de ICANN, nosotros hablamos mucho del uso indebido y qué recursos se deben utilizar. Realmente hemos cristalizado tras el concepto de que cualquier fuente es una buena fuente con tal de que esa fuente sea capaz de ser una evidencia.

Uno de los recursos que se mencionaron tradicionalmente no necesariamente había sido en base a evidencias o que se pueda utilizar como evidencia a tal punto que nosotros como registradores podemos confiar en eso para tomar los pasos que tenemos que tomar. Mucho

del trabajo que se ha hecho en los últimos ocho años literalmente ha sido que la conversación tenga que ver con eso, con tal de que exista una evidencia y si es una acción apropiada que podamos tomar en base a esa evidencia, eso es algo que los registros y los registradores puedan fijarse en esto y de pronto, donde sea apropiado, tomar acción directa o tomar otras acciones.

Creo que es importante que, a medida que nos fijamos en las herramientas para mediciones del uso indebido del DNS o uso indebido en línea, que nosotros tomemos en cuenta ese principio núcleo de transparencia no arbitraria y asegurarnos de que le demos crédito a esos operadores quienes están buscando esos elementos de evidencia, la expectativa de transparencia y cuando se tome alguna acción, que sea algo que se pueda hacer una auditoría o rastrear esa acción. Por qué tomó la acción y en base a qué evidencias. Puede existir información en las evidencias pero queremos asegurarnos de que no estemos ignorando el proceso debido. El reportar un uso indebido no es lo mismo a que existan las evidencias del uso indebido.

NICK WENBAN-SMITH: Gracias. Sea con ICANN o sea que sea con COMPASS o la federación de investigación, todos hacen la diferencia entre gTLD y ccTLD. Quiero entender eso un poco más porque parece que no tiene que ver con el tamaño o con la política de registración. Estamos aquí con Andreas y estamos en la bella ciudad de Hamburgo. Es una zona bastante grande y es bien manejado y seguro, y .UK es similar, es una política abierta de registración bajo precio. Es igual a muchos de los gTLD. Parece que la observación del uso indebido con las tres métricas de pronto no están

de acuerdo pero las tendencias son claras. No es 5-10%. Estamos hablando de una gran magnitud. ¿Por qué es ese el caso? ¿Me lo pueden explicar? He estado pensando en esto bastante y quiero saber la respuesta a eso, por favor.

ORADOR DESCONOCIDO: Antes de contestar, por favor, para los participantes remotos, por favor, digan su nombre para saber quién está hablando.

ORADOR DESCONOCIDO: Gracias por hacérmelo saber.

ROWENA SCHOO: Cuando nosotros estábamos recopilando nuestro informe público estábamos pensando cómo construir esto y cómo incluir los grupos en los TLD. Fue un trabajo retante. Lo dividimos entre gTLD y ccTLD. Cuando estaba escribiendo el texto para cada grupo había mucha variación entre los dos grupos. Hablamos de las variables en los ccTLD pero también existen en los gTLD. Muchos operan en un modelo cerrado. Por ejemplo, .BANK, .PHARMACY. Eso quiere decir que ellos tienen una restricción que es lo que entra y eso quiere decir que tienen restricciones en cuanto al uso indebido también. En alguno de los ccTLD vemos modelos limitantes o restrictivos que de pronto no son tan abiertos hacia los ccTLD. Por ejemplo, nuestros amigos noruegos tienen un modelo muy limitado que limita qué entra.

Con respecto a señalar las razones exactas de por qué hay más o menos uso indebido y qué impulsa esto, me gustaría señalar un estudio importante que está ocurriendo en este momento. ICANN está trabajando en esto con Maciej. Se fijan en estos factores. Cómo los diferentes precios y otros temas influyen cómo se impulsa el uso indebido. De pronto no contesté todas las preguntas pero es algo en lo que empezar a pensar.

NATHAN ALAN: Los estudios que hemos visto parece ser que había más verificaciones colocadas. No sé si esto fue pre o post la registración para entender a nuestros clientes pero parece que fue una combinación lo que aumentaba el uso indebido. Eso es lo que nosotros observamos o que los registros nos informaron de qué es lo que han estado haciendo con respecto a puntos de registración.

NICK WENBAN-SMITH: Samaneh, adelante.

SAMANEH TAJALIZADEHKHOOB: Quería agregar lo que ya dijeron los demás. Creo que como dijo Rowena, lo más importante es que tenemos que encontrar un factor para categorizarlo. A los fines de la presentación, además la regla general es que el espacio de ataque que es aquí la cantidad de dominios, es el factor más crítico, más fundamental para determinar y eso depende del tamaño del TLD y de nada más que eso.

NICK WENBAN-SMITH: ¿Algún otro comentario? Alan. Somos muy malos con la comunicación.

ALAN WOODS: Dos comentarios anecdóticos, por así decirlo. El primero quizá no va a ser de gran ayuda pero quizá los va a hacer pensar. Recientemente escuché hablar acerca de un ataque de uso indebido de DNS específico. Era una campaña que se centraba en dominios bastante costosos. En general la gente piensa que cuanto más económico es, más probable es que lo compren pero a veces se registra un punto de precio que está entre 30 y 60, porque el beneficio que obtengo de los dominios podría potencialmente perderse.

El tema es que los métodos son más sofisticados. Todos acusamos a algunos indicadores muy simples y quizá estos no sean los que deberíamos esperar. Habiendo dicho esto, pienso que igual es un factor de importancia pero hablar en mayor profundidad sobre este espacio nos permitirá ver que no siempre se cumplen las reglas. Tenía un segundo punto para comentar pero por supuesto, como estamos en ICANN, ya no me acuerdo de qué era.

NICK WENBAN-SMITH: Esta mañana en la presentación del GAC se mencionó este tema. Se ha considerado el supuesto de que los dominios más económicos implican un índice más alto de uso indebido pero esto no siempre es así. Tenemos que ser cuidadosos. Es una situación multifactorial. Veo que alguien levantó la mano. Adelante.

ROWENA SCHOO: Creo que mencioné en mi presentación que muchas fuentes que se utilizan apuntan a marcas globales y esto quizá no sea representativo de todos los países y todas las entidades. También he visto que a veces hay ataques de phishing que no están en estas listas pero a veces hay tipos de ataques que no se mencionan, que no surgen en los informes y potencialmente hay una especie de escala en los delitos cibernéticos. ¿Se trata de llegar a la mayor cantidad posible? ¿Es más fácil hacer esto si se utiliza un dominio de alto nivel genérico que es reconocido por gente de todo el mundo? Debería decir que estas son algunas ideas que estamos conversando y debatiendo pero todavía no tenemos evidencias concluyentes.

NICK WENBAN-SMITH: Gracias. Entiendo que lo que está tratando de decir no es que la gente en Alemania sea más honesta sino que a veces la gente usa dominios genéricos de alto nivel porque el mercado al que llegan es mayor.

BART BOSWINKEL: Hay un comentario de John McCormack. Es un comentario con respecto a alguna de las preguntas. Una respuesta potencial tiene que ver con la confianza. Los ccTLD al parecer son TLD de mayor confianza que los gTLD, que tienen mercados globales. La gente se identifica con su TLD local porque es su TLD pero el efecto no es tan común como el que vemos con los gTLD.

NICK WENBAN-SMITH: Gracias, John, por ese comentario. Quería cuestionar alguno de estos puntos. Es cierto que algunos gTLD son realmente genéricos pero también todos sabemos que hay algunos ccTLD que también son genéricos o cuasi genéricos. Estoy pensando en .CO, .ME, .TV, incluso .IT para los italianos. Esto es algo genérico. Uno pensaría que estos nombres seguirían el patrón de un gTLD o de un ccTLD pero creo que no hay evidencias al respecto.

ROWENA SCHOO: Gracias, Nick. Es interesante el punto que señala. Una de las cosas que observamos con COMPASS cuando analizamos las registraciones maliciosas y los dominios comprometidos es que hay un patrón que va surgiendo en torno a los ccTLD y los TLD genéricos que están más comprometidos. Es decir, hay más dominios registrados que parecerían ser legítimos y se convierten. Tuvieron un sistema de gestión que no se actualizó. Hay una vulnerabilidad y por lo tanto el dominio fue comprometido.

Tendemos a encontrar más en los ccTLD y en los viejos TLD genéricos, los originarios mientras que vemos que hay nuevos gTLD que están creciendo mucho y en general el porcentaje de uso indebido es diferente. Hay más malicioso que comprometido. Hay menos dominios durante menos tiempo.

NICK WENBAN-SMITH: Sí. Veamos si lo entendí correctamente. No es que haya menos uso indebido necesariamente en los ccTLD sino que es una clase de uso

indebido diferente. No son necesariamente registraciones maliciosas sino que tenemos muchas registraciones existentes y muchos sitios web antiguos a los que dirigen estos dominios. Quizá no son el objetivo de delincuentes, son sitios web con vulnerabilidades antes que explotación de debilidades en los sistemas de registración.

Esto surgió en muchos debates sobre el análisis de herramientas de gestión. Los números están muy sesgados porque tenemos grandes cantidades de nuevos gTLD. Esto cambia entonces. No estamos necesariamente compartiendo los mismos atributos. Creo que ese es un punto interesante y para nosotros los ccTLD más maduros, más establecidos, creo que obtendríamos mejores resultados si encontráramos formas de contactar a los registratarios cuyos sitios web se vieron comprometidos y si logramos que resuelvan las vulnerabilidades en lugar de hacer que sea más difícil registrar los nombres de dominio. Esa es una idea que se me ocurre.

Hablamos mucho acerca de las listas de bloqueo de reputación antes y quisiera saber lo siguiente. Hay muchas alternativas. Yo soy un poco haragán y prefiero copiar la tarea que hizo otro. Todos vimos estas listas de bloqueo de reputación. Si yo tuviera que comprar una, ¿cuál debería comprar?

ALAN WOODS: No le voy a dar una respuesta directa porque en última instancia yo soy abogado. Para serle totalmente honesto esta es una de las cosas que creo que no hacemos lo suficiente en la industria. Nosotros también tenemos que tener muy en cuenta que la calidad de las diferentes

listas de bloqueo también con el tiempo puede variar. No solamente deberíamos medir el uso indebido sino también en qué medida son transparentes, congruentes o beneficiosas estas listas de bloqueo que nosotros utilizamos. Vuelvo a lo que dije antes. Yo usaría cualquier lista siempre y cuando esa lista me permitiera escalar basándome en evidencias. Así de simple. No me importa si las evidencias muestran que hay un uso indebido en ese informe pero si me importa poder contactar a la parte adecuada para tomar alguna medida.

NICK WENBAN-SMITH: Creo que alguien levantó la mano.

ROWENA SCHOO: Hay mucha variación en las tasas de uso indebido en los ccTLD al igual que hay mucha variación en los gTLD. Nosotros publicamos informes sobre esto, tenemos tablas, los números van cambiando y hay ccTLD que tienen altos índices de uso indebido, ya sea maliciosos o comprometidos. Acérquense a nosotros y vean si sus tableros de control pueden funcionar.

NICK WENBAN-SMITH: Muy inteligente. Está Brian, Bart. Si hay alguien más aquí que quiera hacer una pregunta, indíquenmelo.

BRIAN CIMBOLIC: Quería volver a algo que señaló Alan. Las listas de bloqueo de reputación son importantes y son un indicador importante para

continuar investigando. Sería un error basarse solamente en las listas de bloqueo de reputación. Creo que tener evidencias es muy importante. Les voy a dar algunos ejemplos concretos. Yo tuve proveedores de listas de bloqueo de reputación que me dieron listas de dominios para que nosotros actuáramos y para que incluyéramos no solamente dominios que ya estaban registrados sino dominios que nunca antes habían sido delegados.

Esto no es chiste, alguien también me dio una lista de dominios e incluyó en esa lista el nombre de dominio del proveedor de la lista de bloqueo. Hay distintos niveles de calidad allí. Yo no soy quien puede decir que esto necesariamente está mal pero muchas veces se usan con diferentes fines. Se usan para bloquear redes, para otro tipo de cosas. En general la herramienta no sirve para el propósito que buscamos. Cuando se aplica uno a uno a un nivel de nombre de dominio. No digo que las listas de bloqueo de reputación sean malas pero no siempre están adaptadas para que las utilicemos a nivel del DNS.

SAMANEH TAJALIZADEHKHOOB: Para continuar con lo que dijo Brian, en OCTO tenemos un estudio con 5-10 indicadores de cosas que son medibles en las listas de bloqueo y cosas que son más difíciles de medir. Este documento se va a publicar en la conferencia de e-crime de este año. Les podemos dar esa información.

NICK WENBAN-SMITH: Gracias. Quedan algunas preguntas pero me interesa conocer el trabajo futuro del comité permanente sobre uso indebido del DNS. El sábado yo identifiqué el plan de trabajo para el futuro y una de las cosas que estamos considerando para una reunión en el futuro sería trabajar de una forma un poco más práctica, utilizar herramientas y mediciones y tener un abordaje más práctico. Quisiéramos saber si a ustedes les interesaría esto, si les interesaría quizá tener una sesión sobre herramientas y mediciones. Pueden contactarse conmigo por privado o pueden indicarlo aquí. Quisiera saber si les interesa. El equipo de líderes de este grupo lo consideraría para el futuro. ¿Algún comentario? ¿Les parece que ya resolvimos todos los problemas de métricas y mediciones? ¿O ninguno? Nos quedan cinco minutos. ¿Hay alguna pregunta aquí en la sala? Andrew.

ANDREW BENNETT: Usted dijo que DAAR incluía 22 ccTLD. Creo que hay más de 300 ccTLD. Quisiera saber por qué algunos de los más grandes no están incluidos en DAAR. ¿La ICANN podría convencer a más ccTLD para que se incluyan en este sistema?

NICK WENBAN-SMITH: Samaneh, ¿podría responder esta pregunta?

SAMANEH TAJALIZADEHKHOOB: La respuesta breve es que no sabemos. Estamos volcando esfuerzos para poder avanzar con el proyecto, ver cuáles son los beneficios. Con el tiempo aprendimos que quizá algunos ccTLD tienen

ciertas inquietudes con respecto al archivo de zona que se comparte o que se utiliza. Ya dijimos varias veces que esto no va a ser así. El archivo de zona se utiliza solamente para este proyecto y los informes se envían a los contactos administrativos que tenemos de los ccTLD.

Tal como estamos avanzando con el proyecto, a lo largo del tiempo, es gradual pero está creciendo. Vamos a interactuar con los participantes del proyecto para recibir sus aportes para que el informe sea mejor y para mejorar a lo largo del tiempo. Esperamos lograrlo. Este es el punto al que podemos llegar.

NICK WENBAN-SMITH: Sí. Creo que algunos ccTLD consideran esto. Hablé con otras personas y dicen que reciben tablero de control pero no datos sobre los que poder actuar. Hay algunos requerimientos técnicos y cosas que hay que configurar pero creo que obtenemos un buen retorno. ¿Algún comentario en el chat?

BART BOSWINKEL: Hay dos comentarios. Uno de John McCormack, de HosterStats, que tiene que ver con su pregunta inicial al panel. Dice: La vida útil de la registración de muchos de los nuevos nombres de dominios gTLD es mucho menor que aquellos de los heredados y los nombres de dominio ccTLD. Esta alta tasa de no renovación limita parte de las concesiones que hacemos con software como Wordpress plugins. Este es un comentario de John McCormack. Hay un comentario de Alexander Hugla, de Gandhi. Las listas de reputación privadas creadas

por empresas privadas no son confiables porque tienen un sesgo hacia sus clientes y hacia las acciones que realizan sus clientes.

NICK WENBAN-SMITH: Gracias, Bart. Debo admitir que vi algunas listas de bloqueo de reputación que se comercializan basándose en la cantidad de nombres bloqueos y no en la calidad de su trabajo, de sus investigaciones y sus evidencias, lo cual puede afectar esa decisión de bloqueo. Entiendo el comentario, gracias.

En el último minuto que nos queda quisiera decir que el trabajo del grupo permanente de DNS no se detiene. En las próximas dos reuniones de la ICANN seguiremos hablando de esto. En la reunión de Cancún presentamos los datos de relevamiento de la encuesta y alguien pidió sugerencias con respecto a qué valía la pena seguir investigando. Estas son las cuatro sugerencias de la reunión ICANN 77. Pueden ver que el tercer punto coincide con el tema principal de hoy. Tratamos de devolverla a la comunidad o de darle a la comunidad lo que la comunidad nos pidió. Por eso tenemos este tipo de sesiones. Quiero agradecerles a todos por eso.

Verán que hay otros tres temas. En el equipo de líderes estamos tratando de organizar estos temas para tratarlos a lo largo de los próximos meses para incluir los temas que ustedes piden. Esto no significa que esta lista sea algo fijo. Nosotros respondemos a las solicitudes que nos hacen, si hay algo que quieren agregar o que no les interesa tanto entonces sin duda podemos modificar la lista. Pueden

contactarse con cualquiera de nosotros. Esto es para que tengan una idea de cómo fluye nuestro trabajo.

A mí me interesan en particular ejemplos de colaboraciones entre diferentes registros para que el uso indebido no vaya de un registro a otro. Ya sea un ccTLD o un gTLD, tenemos que tratar de trabajar de forma coordinada. Creo que sería muy bueno ver ejemplos positivos y ver cómo podemos trabajar en forma más eficaz con los registradores. Hay algunos registradores aquí. Es muy bueno verlos. Tenemos que ver cómo podemos trabajar mejor porque creo que todos juntos tendremos más información y recursos para actuar que si cada uno lo hace por su cuenta. Este será probablemente uno de los principales temas en la próxima reunión de la ICANN que tendrá lugar en Puerto Rico. Habiendo dicho esto, son exactamente las… Voy a llegar tarde.

ROWENA SCHOO: Tengo una última información. Hablamos de lecciones aprendidas y cosas que podemos aprender a través de otros registros. A mí me interesaría saber si hay algún esquema de incentivos que tenga impacto sobre los registros, que así pueden manejar mejor a sus registradores. Me interesaría saber si esto existe. No sé si todos los TLD pueden llevar a cabo un programa de incentivos. Quisiera saber si ustedes tienen algún programa así. En ese caso, por favor, ¿me lo pondrían informar? Muchas gracias. Eso es todo.

NICK WENBAN-SMITH: Es una buena sugerencia. Habiendo dicho esto, voy a dar por cerrada la sesión. Muchas gracias a todos por haber contribuido. Nos vemos pronto. Muchas gracias a todos los miembros del panel y a mis colegas. Gracias.

[FIN DE LA TRANSCRIPCIÓN]