ICANN79 | Foro de la comunidad – Sesión plenaria de At-Large organizada por NARALO
Martes, 5 de marzo de 2024 – 4:15 a 5:30 SJU

MICHELLE DESMYTER: Esta sesión va a comenzar. Por favor, empiecen la grabación. Hola y bienvenidos a la mesa redonda de NARALO en la plenaria de At-Large auspiciada por NARALO. Soy Michelle DeSmyter y soy la coordinadora de esta sesión. Por favor, sepan que esta sesión está siendo grabada y se rige por las normas de conducta esperadas de la ICANN. Los comentarios y preguntas serán leídos en voz alta una vez sean presentados en el espacio correcto en Zoom. Si quieren hacer una pregunta, levanten la mano en Zoom. Les daremos permiso a los participantes para que abran su micrófono en Zoom.

La interpretación será en inglés, español y francés. Por favor, digan su nombre para que conste en acta y el idioma que va a hablar si va a hacer su intervención en un idioma distinto del inglés. Por favor, hablen a un ritmo razonable. Con esto le doy la palabra a Greg Shatan, presidente de NARALO.

GREG SHATAN: Buenas tardes. Bienvenidos a la mesa redonda de NARALO. Como saben, es una tradición de At-Large que NARALO, que es la RALO anfitriona, no solamente somos anfitriones para esto sino para dos conversaciones de paneles diferentes, y este es uno de esos y este es el momento para discutir un tema de mucho interés actualmente que se

ha dado desde hace mucho tiempo, desde el inicio de Internet, aunque en aquel entonces había uso indebido pero no era del DNS.

Tenemos un panel muy distinguido con nosotros el día de hoy. En orden, desde mi derecha, tenemos a Laureen Kapin, que es la subdirectora de protección al consumidor a nivel internacional. También trabaja en el grupo GAC de seguridad pública. También tenemos a Graeme Bunton, que es el director ejecutivo del Instituto del Uso Indebido del DNS. También tenemos a Steve Crocker, quien no necesita presentación alguna. Pueden leer sobre él en muchos lugares. Es un placer y un honor tenerlo aquí, en este panel. Una de las muchas cosas que yo admiro de Steve es que nunca termina de aprender y de buscar temas nuevos. Tiene un gran enfoque sobre el uso indebido del DNS. No hay nadie con mayor credibilidad en este tema que Steve. Puedo sentir cómo gravita todo en torno a él en este tema. Él es presidente y director ejecutivo de Edgemoor Research Institute Incorporated.

Tenemos también a Ram Mohan, que es el oficial jefe de estrategias de Identity Digital. Tenemos el placer de tener a Ram con nosotros. Tenemos a Reg Levy. Ella acaba de tomar asiento. Estoy haciendo que se levante de nuevo. Tiene que caminar con su café, su computadora, su mascarilla. Es la jefa de cumplimiento para Tucows. Es alguien que también ha estado arando durante años el jardín de la ICANN.

Tenemos este panel tan distinguido hoy para discutir lo que es el uso indebido del DNS y de los dominios en la economía digital. Dado que este es un panel que va a hablar desde la perspectiva del usuario final, desde la perspectiva At-Large, esperamos que sea tomada en cuenta

esa perspectiva durante la conversación. Se han dado muchas conversaciones en esta reunión de la ICANN sobre el uso indebido del DNS. Hemos visto varios sucesos interesantes que se han dado recientemente. Uno es el RDRS. También las modificaciones a los contratos de partes contratadas. También tenemos después de muchos años una definición ya consensuada de lo que es el uso indebido del DNS. Ya no hay que reinventar la rueda como lo hacíamos antes.

Aunque tenemos aquí un orden y veo que Steve Crocker tiene una C mayúscula junto a su nombre, voy a empezar con Graeme Bunton, como director ejecutivo del Instituto del Uso Indebido del DNS, dado que su vida profesional completa está dedicada a este tema. Quisiera escuchar sus impresiones y empezar con su intervención.

GRAEME BUNTON: Gracias, Greg. Es una apertura bastante amplia. Soy Graeme Bunton, como mencionó Greg. Creo que aquí lo clave que hay que rescatar, creo que voy a empezar con el tema de las enmiendas o las modificaciones, es que entran en vigencia el 5 de abril. Tenemos que estar atentos a eso y crean obligaciones claras para los registradores y registratarios dado que se define lo que son registros maliciosos.

Creo que el futuro es muy brillante para el campo de la lucha contra el uso indebido del DNS, siempre dependiendo de las herramientas que ahora ha implementado o que ha creado la ICANN. Yo estoy muy ansioso de ver cuándo entra en vigencia todo esto. Creo que va a cambiar mucho el panorama del uso indebido del DNS. Creo que va a

ser algo que sirva para informar mucho sobre el trabajo que se realiza aquí. Va a cambiar el panorama de Internet como tal, creo.

Quizá es una idea un tanto capciosa pero no estamos aquí para resolver el ciberdelito ni tampoco vamos a detener aquellos malhechores que tienen la intención de hacer cosas indebidas. Lo que sí vamos a hacer es que vamos a regular todo un poco más y eso quizá va a cambiar la forma en como actúan estas personas que actúan dolosamente. ¿Qué van a hacer? ¿Se van a ir hacia otros sitios que estén más comprometidos, donde puedan explotar más servicios? ¿Se van a ir a otros subdominios, se van a ir a otras rutas alternas? Los efectos secundarios de estas modificaciones creo que van a ser muy interesantes. Quizá esas son preguntas picositas para empezar a pensar sobre esto pero creo que es importante considerarlo.

GREG SHATAN: Gracias, Graeme. Creo que con eso empezamos bien. Lamento que no vayamos a resolver el ciberdelito pero una constante es que los villanos siempre están un paso adelante de los chicos buenos y es por eso que los chicos buenos tienen que seguir en movimiento siempre. Hablando de eso y hablando de cumplimiento, vamos ahora a hablar con Laureen Kapin, nuestra próxima expositora. Sé que Laureen tiene algunas diapositivas. Muy bien. Me preocupaba que al estar fuera de orden iba a atrasar todo. Adelante, Laureen.

LAUREEN KAPIN: Soy Laureen Kapin. Estoy hablando en mi condición de copresidenta del grupo de trabajo de seguridad pública pero también como subdirectora de los asuntos de protección del consumidor en la Comisión Internacional de Comercio. Verán en la siguiente diapositiva el nombre de oficina. Algo que sí quería hacer era darles una perspectiva mundial real sobre cómo se da el uso indebido del DNS en el mundo y cómo constituyen un tipo de fraude.

Estas son estadísticas del 2023 en cuanto a las denuncias de fraude que hemos recibido. Solo como antecedentes y para aclarar, estas estadísticas de fraude no son equivalentes al uso indebido del DNS que es algo que tiene una definición taxativa y muy puntual en el mundo de la ICANN. Estas son estadísticas de fraude que generalmente la Comisión Federal de Comercio recopila porque sabemos que las autoridades del orden de Estados Unidos encargadas de proteger al consumidor recopilamos estos datos y tenemos muchas denuncias que se presentan en todo Estados Unidos presentadas por los consumidores, por las víctimas, por los better business bureaus que son como las oficinas de protección al consumidor y por otros actores. Esto nos permite compartir estos datos con el público.

Con referencia al nombre de la oficina que es la Comisión Federal de Comercio, tiene que ver más que nada con la parte de aranceles y no tanto con la parte de importación y exportación. Muy bien. Aquí vemos los puntos más importantes. Básicamente estamos tratando de ver cómo resulta el uso indebido del DNS o cómo impacta al usuario final, que son personas como ustedes y como yo que usamos los DNS.

Los reportes están aumentando. Recibimos 2.6 millones de denuncias por fraude el año pasado. En cuanto a pérdidas, estas son pérdidas en dólares americanos fuera de otro tipo de daños como el daño emocional y demás que son otros daños o perjuicios que sufren las víctimas. Estamos hablando de una pérdida de 10.000 millones de dólares por estos delitos. También vemos que hay el fraude de impostores. Esos son impostores que se hacen pasar por negocios o por personas. Uno de los temas discutidos aquí, en la ICANN, es el de dominios que se utilizan para hacerse pasar por negocios legítimos y que no lo son. En cuanto a los métodos de contacto, el más popular, diría yo, por falta de una mejor palabra, el método de contacto más popular es el correo electrónico. Ese método es de enfoque particular dentro de la comunidad de la ICANN.

Aparte de la pérdida económica en dólares lo que también señalamos en estas estadísticas es que las personas están perdiendo mucho dinero cuando se trata de fraudes de inversión. Cuando pensamos en las áreas en las que se dan los fraudes está la parte de fraude por inversión, especialmente cuando se trata de criptomoneda. Recordemos que la categoría principal es la de las estafas de impostores. Luego tenemos el de compras en línea, el de premios, rifas, loterías, etc., los de inversiones y los de oportunidades de empleo.

Ya sabemos también que hay diferentes métodos de contacto. Sabemos que los correos electrónicos son los más populares inmediatamente seguidos de llamadas telefónicas y mensajes de texto. Si vemos cuál representa una mayor pérdida económica reflejándolo

en dólares vemos que son la parte de redes sociales, los anuncios en línea y también los sitios web.

Finalmente, quiero hablar de phishing, que es un tipo de uso indebido de nombres de dominio. Desde marzo de [2024] hemos recibido más de 1.000 reportes, casi 100 en el último mes, por phishing que representan una pérdida equivalente a 2.2 millones. Nuevamente vemos que eso se relaciona con el servicio o con el método de fraude que es de impostores de negocios, que es algo que también está siendo discutido ampliamente.

Con esto me voy a detener para ver nuestros datos. Si pueden ir a la última diapositiva, si quieren ver información detallada de los datos que tenemos publicados, les exhorto a que vean nuestro libro de datos del 2023. También la data pública porque pueden ver la comparación de año con año, trimestre con trimestre. Pueden ustedes comparar métodos de contactos y otros temas. Pueden ustedes hacerlo todo en tiempo real. Es un recurso muy interesante para conocer más sobre estas cifras y estadísticas.

Lo que quiero resaltar aquí es que muchas veces estamos pensando: "¿Cómo puedo definir esto? ¿A quién puedo reportárselo?" Esos son temas muy, muy importantes para que los puedan revisar. No podemos perder de vista tampoco el impacto que tiene esto sobre el usuario final, que es en realidad la víctima verdaderamente en todo esto. Muchas veces pierden los ahorros de toda una vida, su jubilación, sus casas a razón de estas estafas, de estos fraudes.

Sé que suena un poco dramático y muy exagerado para algunos pero lo tengo que poner así, en perspectiva, para que veamos todo el daño que se puede hacer con estos delitos que puede ser algo que va desde que no hay ningún tipo de pérdidas porque el usuario está bien versado en la materia hasta alguien que puede perderlo todo porque no conoce al respecto. Me detengo ahí.

GREG SHATAN: Gracias, Laureen. Esas son estadísticas muy interesantes. Ahora vamos a escuchar a Ram Mohan, alguien que tiene el mismo nombre que la memoria de la computadora. Ram, ¿algo que quieras compartir sobre todo esto, especialmente con la definición que hemos dado del uso indebido del DNS?

RAM MOHAN: Muchas gracias, Greg. Quisiera centrarme en los temas que se llevan a cabo. Cuáles son los problemas que tenemos que considerar. No es la incidencia del uso indebido. Ni siquiera la mitigación del mismo sino el momento de la mitigación del uso indebido. En mi mundo probablemente sea la métrica más esencial y más crítica a evaluar. Si se pone como ejemplo el phishing, que es un problema que nos afecta a todos en nuestra vida diaria, la diferencia en el impacto negativo de encarar una campaña de phishing, la diferencia entre eliminarla en las primeras seis horas de haberse enterado del tema hasta la primeras 16 horas, con una diferencia de 10 es un orden de magnitud.

Literalmente, con este tipo de cosas, estas son implicancias prácticas cuyo foco, entiendo, tiene que estar no en la cantidad de veces que sucede algo, la frecuencia en que sucede, sino que el foco debe estar no tanto en el volumen o en el tiempo medio para eliminarlo. Tenemos que considerarlo como industria. Como grupo de la comunidad tenemos que buscar la mediana del tiempo de su eliminación.

Tenemos que centrarnos una y otra vez en eliminarlo. ¿Cómo hacemos que esto suceda? Dentro del mundo de la ICANN mucho de esto termina afectando a los registros, a los registradores. Si hicieran un poco más, si hicieran algo adicional. Pero hay otra parte del uso indebido del DNS en el que el uso indebido requiere contexto. Hay determinado tipo de cosas que parecieran abusivas desde el punto de vista del contenido pero en el contexto no es así. Sí se instalan algoritmos automáticos que buscan ciertas frases que suenan como discurso de odio o que se centran en delitos. Las consecuencias imprevistas de este tipo de medidas automatizadas provocan la eliminación de trabajos técnicos. Terminan en sandboxes, en trampas que se eliminan. Ese es el segundo punto que quiero resaltar. Considerando el contexto del uso indebido del DNS, yo diría que es prácticamente tan importante como el contenido en sí.

El último punto es que a menudo en este ecosistema consideramos a las partes contratadas, aquellas que tienen que realizar cambios positivos sobre el uso indebido para ayudar a que el ecosistema sea más seguro desde un punto de vista relativo. Hay toda una serie de actores aquí. Creo que tenemos que buscar maneras de llegar a ellos para comprender lo que están haciendo. Empresas que brindan

hosting y otros proveedores. A veces verán que hay algunas cosas que claramente parecen uso indebido, se presenta la solicitud al registro, puede llegar inclusive a la ICANN que dice: “Vaya al registro”, va al registro y el registro dice: “Vaya al registrador” y el registrador dice: “En realidad vaya al proveedor de hosting porque esto es un tema orientado al contenido”. Tenemos que encontrar una manera de incluirlos en el conjunto de soluciones. Al principio del diseño de las partes involucradas de la ICANN, este tipo de proveedores a menudo no estaban sentados a la mesa. Hacían cosas buenas. Había muchas que hacían cosas buenas pero sus mejores prácticas no eran buenas en lo que estaban haciendo.

El punto final que quisiera comentar. Como dice Graeme, la meta no está allí para evitar sino mitigar, número uno. Número dos, dentro de nuestro sistema, si hay cosas claras y explícitas que podemos hacer para responder con mayor rapidez, para eliminar el mal comportamiento tenemos que hacerlo.

Dentro de nuestro propio registro tenemos un programa experimental que no hicimos en un ambiente de producción pero estamos probando un programa experimental donde se registran los nombres de dominio. En el momento del registro o registración, el registro tiene la identificación real del registratario. Muchas veces, más del 60% de las veces, está oculto detrás un proxy pero se pueden ver los patrones y las firmas de quien se presenta, las cadenas de caracteres que utilizan.

De alguna manera lo bueno es que los delincuentes también se vuelven vagos y si encuentran un mecanismo que funcione terminan apostando más sobre el mismo. Nosotros, como responsables,

tenemos que tener programas que identifiquen ese tipo de patrones de holgazanería y hacer algo al respecto.

Tenemos un experimento en nuestra empresa por el cual si al momento de la registración se puede discernir que haya una posibilidad de que un nombre o un grupo de nombres registrados, puede que no tengan intención pero sí un patrón similar a patrones exhibidos previamente, eso tiene intención maliciosa clara en cuyo caso ponemos esos nombres en una lista de vigilancia. Si se identifica que hacen uso indebido de los DNS, el momento para eliminarlos, si lo logramos en una hora en lugar de seis o siete horas, si lo logramos desde un principio, el orden de magnitud es dramáticamente superior lo antes que podamos eliminarlos. No tiene uso ya para los delincuentes que lo están haciendo. Me baso en cosas prácticas tratando de traer a los que no están a la mesa como parte de involucrar a la ICANN.

GREG SHATAN: Muchas gracias, Ram. Mucho para pensar. Tenemos que pensar cómo traer a estas partes a la mesa y que todavía no están aquí. Quizá eso cambie. Quisiera pasarle la palabra a Steve Crocker que creo que tiene cosas interesantes para decir. Muy bien. Van a ser interesantes.

MICHELLE DESMYTER: Un momento, Steve. Un segundo, por favor.

STEVE CROCKER: Vengo trabajando en un área que es adyacente a los problemas de uso indebido del DNS. Hay áreas de similitud y superposición que van a tener cada vez más influencia. Esto lo llamo el lío de WHOIS, que tiene que ver con los registros, los datos de registro, la recopilación de estos datos, lo que se recopila y cómo se debe manejar y cómo tener acceso a esto. Esto es un proyecto que llamamos Jake, por Jake Feiler, que fue la persona original en el WHOIS. Quisiera ver mis diapositivas. Aparecen y se van.

GREG SHATAN: Disculpas por las dificultades técnicas.

STEVE CROCKER: En breve, desde hace muchísimo tiempo, medido en décadas, he visto intentos repetidos de tratar de resolver el tema de cómo manejar los datos recopilados, cuáles recopilar, especialmente en la estructura de la ICANN, repetidamente. Cuando me fui de la junta, al final del 2017, no habiendo logrado estimular lo que pensé que era un curso útil, yo personalmente y otros pasamos a colaborar de manera lateral y a pensar en este problema en profundidad.

Elaboramos una serie de ideas trabajando mucho para difundirlas y que se implementen. A la vez, estuve participando en debates internos de los procesos de desarrollo de políticas fase 1 y fase 2, del proceso de desarrollo de políticas expeditivo y también del servicio de datos de registro.

¿Qué sería éxito aquí? La idea sería tener un sistema que logre privacidad, exactitud y eficiencia. Probemos la siguiente. Probamos sin diapositivas, parece. Muy bien. Muchas gracias. ¿Podemos tener la siguiente diapositiva? Eso es un desafío. La respuesta es sí podemos pero hace falta esfuerzo. El trabajo realizado a la fecha es bastante plano en el sentido de que ha habido debates largos sobre cosas sencillas y no llegamos a las difíciles y las cosas difíciles nunca se resuelven.

¿Qué pasa con GDPR? Esto fue una pelota que entró y pateó todo para el lado pero cambió el nivel de detalle en una atención hacia la privacidad pero con problemas en decisiones de distintas sutilezas. Considerando una mirada fresca, no voy a entrar en detalles del tema, podemos hablar de esto porque puedo poner las diapositivas a su disposición, así que obviemos los detalles.

Aquí vemos los registros de nombres de dominio. Esto está simplificado en el sentido de que tenemos el registro arriba, la base de datos, el registrador, los datos entran al registrador y aquí entran en producción desde el registratario abajo a la derecha y a la izquierda arriba tenemos la gente que hace solicitud de datos. Esto era relevante antes de GDPR. Veamos. Sigamos, por favor. Este es el WHOIS legado. Avanzamos.

Las cifras que entiendo estaban en el orden de 5.000 millones de consultas por mes previo al GDPR. Es una cifra grande en todo el sistema. Cuando se preguntan las cifras hoy, están divididas entre información pública y las consultas de información no pública que sí recibimos dos o tres y las cifras son tan distintas. Nos hacemos

preguntas de cómo eran las consultas antes. No eran necesarias y había ruido blanco. Me cuesta explicar los múltiples órdenes de magnitud. De dos a tres quizá pero el doble es demasiado.

Venimos armando un modelo abarcatorio. Una parte de ese modelo es cuáles son las reglas de los datos recolectados y cómo se etiquetan en términos de sensibilidad, elementos de datos, precisión, etc. Reconocemos aquí que cuando hablamos de cuáles son las reglas para esto todos tienen una opinión. A veces hay reglas realmente firmes. Los registradores, los registratarios, los gobiernos pero todo esto interactúa con lo demás. Algunas son más explícitas, documentadas y claras. Cuando uno las desglosa encuentra que el registrador puede querer hacer algo pero está vinculado con el registro y ambos con las distintas autoridades que están operando y no hay una garantía prioritaria de que sean uniformes y consistentes. Tenemos reglas europeas y de Estados Unidos y podemos encontrar que en ciertas instancias no se puede cumplir con ambas porque sus requisitos no son equivalentes. Lo importante es documentar las reglas. No es que tengamos que hacer con la especificación de lo que debería ser. Podemos documentar de qué se trata o lo que dicen que trata y mostrarlas de manera muy vívida y clara para verificar si son coherentes entre sí o no.

Del lado de las solicitudes tenemos distintos matices de los datos seleccionados, de las circunstancias. Podemos decir que no es el momento para ver los detalles pero es posible lograr mucha precisión desde ese punto de vista. Por ejemplo, trabajamos muy cómodamente con Lorraine, Gabe y otros del grupo de trabajo de seguridad pública.

¿Qué tipo de consultas quiere que se hagan y en qué circunstancias? Voy a dejar en la próxima diapositiva una imagen sobre ese tema. Tenemos plantilla de solicitud. Vamos a pasar rapidito todo esto. Siguiente, por favor. Una hacia atrás, por favor. Aquí tenemos algo crítico. Estamos en una era en la cual se nos dice que todas las solicitudes de datos no públicos tienen que ser examinados para ver si tienen equilibrio con texto, legitimidad de propósito y demás.

Eso requiere un abogado calificado porque los riesgos son tan enormes con cada solicitud… Esto no tiene sentido para nada. Si uno dice: ¿De qué se trata? ¿Qué es lo que busca? Una y otra vez. ¿Qué datos quiere para tomar esa decisión? Esos datos no se recopilaron y están en el sistema como prioridad. No van a poder pedir al registrador en tiempo real que le brinde esa información y que responda más preguntas.

Creo que prácticamente todas las consultas que se van a hacer y todas las decisiones que se toman se pueden tomar de rutina en una organización sensata. Se logran múltiples cosas con eso, reducir el costo enormemente, el tiempo que lleva lograrlo enormemente. Otra cosa es que se incrementa la uniformidad y la transparencia del proceso.

El proceso se transforma de algo del siglo XIX a algo del siglo XXI que debería ser el punto de partida. Parte de esto involucra establecer las reglas del juego. Este es uno de los ejemplos típicos de propiedad intelectual. Se va a hacer alguna serie de solicitudes. Si van a hacer una solicitud en representación de un cliente, las normas van a ser tales en términos de la relación, los problemas que pueden surgir y los riesgos, si se miente con estas cosas y sabemos dónde encontrarlo, por ende, si

usted se registra, es respetable y lo podemos auditar, procede con mayor rapidez y nosotros, el registrador, quizá puede avanzar con mayor rapidez y las cosas tienen un buen ritmo. Hay acuerdos similares. Esto repite lo que les decía al principio. Cada solicitud se verifica en la práctica y mucho de esto puede ser automatizado. Voy a cortar aquí y volver con el uso indebido del DNS y otros temas.

Una parte importante de este tipo de transacciones que estábamos imaginando comparten mucho con el proceso de eliminación por uso indebido del DNS. Quién hace la solicitud, qué información se entrega, qué documentación se entrega, quién queda en riesgo si hay una situación de uso indebido y demás. Hay una serie de maquinaria potencialmente compartida subyacente de todo esto. Esta es la lección que quiero dejarles en este momento.

GREG SHATAN: Gracias, Steve. Algo que escuché de ti y de Ram era el tema de la preocupación por el tiempo, el tiempo para mitigación, el tiempo para la información. Creo que ese es un aspecto crítico de todo esto. Recuerdo que estábamos pensando en crear una máquina para remplazar a WHOIS y ahora tenemos otra máquina básicamente que es el RDRS. Ahora le damos la palabra a Reg Levy, de Tucows. Por favor, adelante.

REG LEVY: Gracias. Gracias por permitirme ser la última porque me permite contestar algunas preguntas que hicieron o alguna de las inquietudes.

Realmente me gustó mucho la apreciación de Ram. Dijo que había una necesidad de tumbar esto rápido. Sí es así pero también tenemos que poner en la balanza el daño que se hará hacia los registratarios y el daño que se causa cuando un dominio que ha sido comprometido sigue en el aire. Yo no tengo los datos para ver cuántos de estos dominios que hemos ubicado son creados con esa intención maliciosa o dolosa. Hay que saber también qué tan fácil es contactarlos. ¿Van a creernos cuando nos acerquemos a decirles que pasa algo malo con su sitio web?

No simplemente se trata de bajar dominios. Se trata de sacar a empresas del aire y hay que entender eso. En Tucows trabajamos con los proveedores y estamos buscando la manera de identificar patrones. Han dado mucha información sobre el registro de datos porque pensé que estábamos hablando del uso indebido del DNS. El otro tema que puedo mencionar es cómo se correlaciona esto con un determinado actor.

Nosotros en Tucows no vamos a bajar todos los dominios del aire. Lo que vamos a hacer es bajar quizá dos con nosotros, dos con otra empresa y así. A veces puede que utilicen datos robados de personas reales pero no va a ser la persona que está detrás del dominio. No están registrando a Mickey Mouse sino que están registrando Reg Levy y usando la información que yo puse en algún lugar.

Esa información de la dirección de IP es una pieza de información mucho mejor y que ayuda a luchar contra un ataque doloso en curso porque es allí donde se está trabajando. Dije que estábamos trabajando interna y externamente. Hay diferentes maneras de

sincronizar la información que reciben los nombres de dominio y lo que nosotros podemos obtener con una dirección de IP.

Podemos decir: “Hey, GoDaddy”. Vimos esta etiqueta en nuestra red y aquí hay datos adicionales correlacionados con un nombre de dominio que está registrado en tu sistema. ¿Puedes por favor ver ese dominio y decirnos si se puede tomar alguna acción o no? Obviamente es algo que se hará en el futuro pero estamos ya viendo esto porque no hay nexo entre los datos de registros y el uso indebido del DNS.

La pregunta es cómo puede el RDRS evitar que se dé el uso indebido del DNS. El RDRS debe decirle a la junta qué tipos de registros o solicitudes estamos recibiendo. Estas solicitudes que hemos recibido no tienen que ver con el uso indebido del DNS sino con el uso indebido de direcciones completas.

Aquí Steve mencionó que sería genial si a los solicitantes se les dice qué información es necesaria de forma tal que puedan darla en un formato estandarizado y luego se puede repasar con mucha facilidad. Eso es lo que hemos hecho. No necesariamente el uso indebido del DNS. Lo hemos hecho con educación, dando toda la información que necesitamos y luego hemos procedido a evaluar cada uno por separado porque no siempre es fácil.

Como abogada me especializo en propiedad intelectual. Creo que el hecho de que alguien tenga un trabajo no necesariamente significa que vaya a tener acceso a un nombre de dominio en particular y los datos del WHOIS. Siento que estoy hablando de todo un poco porque

estamos hablando del uso indebido del DNS y yo estoy hablando ahora de los datos de WHOIS.

.CN tiene una de las políticas de registro más estrictas que hay en la industria. Realmente tiene una de las cantidades de uso indebido más altas del DNS. Es porque es .COM. Hay mucho phishing utilizando .COM porque es lo que es la norma principal, usar .COM. También esto es parte de este ecosistema porque hay mucho fraude en Internet y mucho de ese fraude viene porque antes la información de WHOIS era pública. Eso era muchísima información a disposición del público como por ejemplo correo electrónico, la dirección física de alguien, los nombres. Esta era información de los registratarios que son usuarios finales que han registrado otro producto. No hay una visión unilateral particular de cómo mi equipo puede tumbar un DNS una vez que ha sido utilizado indebidamente.

GREG SHATAN: Gracias. Nos has dado mucho para pensar, Reg. Si hay alguien que tiene alguna pregunta en el panel, puede levantar la mano. Si alguien quiere agregar algo nuevo a la conversación. De no haber preguntas o respuestas o intervenciones, entonces yo voy ver en el pod. Veo que Laureen levantó la mano.

LAUREEN KAPIN: Dado que hablé de las estadísticas horribles, también quiero decir que tengo ciertas apreciaciones sobre lo que hemos dicho. Creo que básicamente lo del uso indebido del DNS y estos mecanismos para

luchar contra esto son herramientas o formas muy proactivas en las que se ha afrontado a estos actores malhechores. Otra manera también es las métricas que obtienen los colegas del instituto del uso indebido del DNS y con eso podemos guiar, informar y renovar los esfuerzos en materias de política para futuro.

Estamos buscando renovar la información más granular a nivel de registrador y registratario. También quiero escuchar sobre el trabajo que están haciendo los registradores y registratarios para poder alentar a estos registradores y registratarios de manera más proactiva en lugar de siempre tener que esperar que haya una queja presentada. Creo que es una manera, un modelo, donde la comunidad puede participar de manera muy entusiasta, con mucha energía y tratar de ser proactivos en lugar de ser reactivos ante las situaciones que se puedan presentar o ante una crisis. Quería agregar estas acotaciones.

GREG SHATAN: Gracias, Laureen. Antes de darle la palabra a Reg quisiera hablar de si no hay relación entre el uso indebido del DNS y los datos de los registros. Sabemos que el uso indebido del DNS es algo por sí solo. No hay relación entre los datos del WHOIS y los datos del RDRS y la mala actuación en sí misma.

Cuando estamos buscando una actuación indebida o equivocada tenemos que buscar el WHOIS y todas estas migajas o datos que nos van dando información sobre esa actuación indebida que estamos tratando de investigar. Tenemos que hacer esto en la medida en que

vamos recopilando las herramientas para ir dándole seguimiento a esto. Adelante.

REG LEVY: Gracias, Laureen. Muchísimas gracias. Cuando tratamos de hacer todas estas cosas para perseguir a los actores dolosos que hacen todas estas cosas para lograr el uso indebido del DNS vemos y recordamos todos los esfuerzos que se han hecho para que esto se dé y pensamos en cómo va a cambiar el panorama debido a estas nuevas medidas y esperamos que la ICANN las implemente. Veremos qué pasa en ese terreno.

Esto es lo que está haciendo la comunidad. Esto es lo que están haciendo las partes que han sido contratadas y queremos ver qué sale de estas modificaciones porque sabemos que vienen unos próximos pasos y queremos saber qué es eso. Sabemos que los malhechores siempre están solamente un paso adelante. Estamos tratando de recopilar datos con estos esfuerzos que hemos realizado. Estoy ansiosa de ver cuáles serán los resultados. Sé que podemos avanzar a partir de esos datos.

GREG SHATAN: Gracias, Reg. Graeme, en un momento voy contigo. Graeme y tú hablasteis de cumplimiento. Me siento muy triste de no tener a alguien de cumplimiento aquí, en este panel, porque ellos tienen el arsenal. El tema aquí es si tienen el valor, la garra para afrontar todo esto y afrontar un paradigma diferente de cumplimiento. Vimos que han

tomado pasos de bebé a lo largo de los años pero obviamente no tenían lo que necesitaban pero ahora sí. Todos vamos a estar muy vigilantes para ver cómo se dan las cosas en este sentido. Graeme.

GRAEME BUNTON: Gracias. Unas cuantas cosas sobre las cosas que se dijeron. En primer lugar, cuando vemos la parte de cumplimiento del lado de las partes contratadas creo que les hemos dado lo que necesitan. También viendo la parte de los reportes individuales creo que han obtenido lo que necesitan. También pensando en nuestro programa de cumplimiento y el otro proyecto de métrica de la ICANN, creo que les va a dar lo que necesitan para que tomen las acciones necesarias.

De mi lado, toda la comunidad, los registrantes, los registratarios, ALAC, GAC, todos tienen que hablar el mismo idioma. Me siento muy optimista de que van a utilizar esto. Podríamos pasar muchísimo tiempo hablando sobre la diferencia entre cómo se puede mitigar el uso indebido en la precisión de los datos de registrador o registratario. Creo que aquí básicamente vemos cómo en el instituto y en otros lugares se han mantenido al margen de la precisión de esos datos porque cuando hay uso indebido de estos DNS, hay gente que dolosamente está tratando de utilizar indebidamente un nombre de dominio. Ese uso indebido del dominio no requiere de datos. Esto es cuando es phishing.

Hay muchas personas que cuando hacen los registros lo hacen libres de PII pero creo que tenemos que considerar esta última parte que para mí es muy importante en la medida en que el instituto ve el

trabajo realizado y pensamos cómo podemos hacer una diferencia en el uso indebido del DNS. Creo que hay dos maneras de hacerlo. Primero, podemos ser más proactivos. Podemos hacer los reportes de manera más precisa y de manera tal que la información llegue más rápido a quienes les tiene que llegar. Así es como vamos ponderando las modificaciones para evitar ser tan reactivos.

Recuerdo que Ram estaba hablando del trabajo alfa y el trabajo beta, sea lo que sea eso. Estamos hablando de aprendizaje por máquinas. Creo que hice una presentación en el simposio de Vietnam, si hay alguien que tenga curiosidad. Brevemente, aquellas personas que han publicado un trabajo sobre el aprendizaje en máquinas, también lo de los DNS y el uso indebido de los mismos, creo que lo han hecho para no hacerlo a nivel comercial. Muchas veces no tienen suficientes datos para construir un modelo que sea lo suficientemente funcional. Creo que los registradores están más equipados para tener más tecnología e identificar los nombres de dominio antes de meterse en una determinada zona y potencialmente causar daños. Eso no es lo que queremos. Queremos evitar causar daños para empezar.

Luego tengo una pregunta que puedo discutir con alguien más que esté interesado porque a mí me interesa. ¿Tiene sentido invertir en ese modelo? Se está viendo como una obra de ingeniería muy, muy complicada o simplemente usamos a los procesadores de pagos que ya usan estas medidas antifraudulentas entre otras herramientas. Creo que esa quizá sea una tecnología más inmediata, más fácil de integrar. Es más fácil que tratar de construir nuestros propios modelos que sean

sofisticados. Creo que eso es algo que hay que considerar. Me detengo aquí.

GREG SHATAN: Esto me recuerda algo que me dijo un registrador hace tiempo. No nos importa WHOIS. Tenemos bases de datos propias y metodologías. Eso se vincula con la industria de tarjetas de crédito, su metodología. Eso tiene sentido y creo que la separación entre el quién y el qué, el uso indebido del DNS es el qué y no hace falta el quién para ocuparse del qué. Por supuesto, hay una serie de cosas malas que pasan pero fundamentalmente el foco tiene que estar en el qué. En segundo lugar, distintas maneras de encargarnos del quién. Steve.

STEVE CROCKER: Interesante. Un par de comentarios. Cuando pienso en términos de datos de registro no tengo en mente qué es exactamente lo que se recopiló o lo que es accesible a través de RDRS. Yo creo que incluye información de pago, el titular de la tarjeta y una variedad de atributos, los cuales se recopilan durante el momento del registro.

Sobre el titular de la cuenta. Seguramente algunos habrán registrado algún nombre de dominio. Hay una distinción clara en el proceso por el cual uno se involucra para tener el nombre de dominio. Hay una cuenta e información de tarjeta de crédito normalmente. Se selecciona el nombre que uno desea y, si está disponible, lo registra y asigna el registrador. Después de tener la autoridad formal sobre el nombre, la

tiene el registrador pero el control físico del nombre es la persona que puede ingresar con la cuenta y hacer cambios en segundos.

Los titulares de las cuentas no se mencionan en ningún momento, en ningún lado. Son una relación entre el registrador y el cliente del registrador. No aparecen en el WHOIS ni delgado ni amplio. Como les decía, es una visión más abarcatoria y dada esta algunas de las preguntas que uno se haría para buscar patrones se tornan más relevantes y de gran importancia.

Respecto a los patrones, otro elemento. Una cosa es mirar los datos dentro de un registrador particular y otra es buscar en todo el ecosistema. Imagínense que esta declaración causa algunos comentarios que hicimos con la privacidad, con la inversión necesaria para crear esto. Les puedo decir que sí, que entiendo esas reacciones pero no es simplemente que esto crea un problema gigantesco. Sabemos cómo construir y controlar ambos sistemas y podemos hacerlo si queremos hacerlo.

Me gusta mucho el comentario sobre utilizar los controles y mecanismos de la industria financiera y también sus procesos. Se verifica la tarjeta de crédito en lugar de aceptarla. Hay herramientas muy sofisticadas para decidir si la tarjeta es buena para el propósito de ese momento. Hay una serie de cosas. Son reacciones rápidas a las cosas que se han dicho aquí.

GREG SHATAN: Reg tiene la mano levantada.

REG LEVY: Gracias. Me impresiona la cantidad que se ve de ataques, si se publicara o si se distribuyera la información de los clientes como parte de una solicitud de datos de registro. Quiero volver a alguna de las otras preguntas que se nos hacen sobre si la ICANN tiene un papel que jugar en el uso indebido del DNS. Me sorprende esta pregunta. La ICANN no se ocupa del contenido. Punto. Podemos hablar de lo terrible de CCM y lo que hacen los registros, los registradores. Lo hacemos todos los días pero no hablamos de eso aquí porque no está dentro del mandato ni del alcance de la ICANN. Preocupa que se pida que la ICANN extienda su alcance en ese sentido.

Si la ICANN tiene que publicitar su papel en uso indebido del DNS, sí, creo que es bueno. Mucha gente ha escuchado hablar de la ICANN. No sabe de qué se trata lo que hacemos. Sería muy bueno en ese sentido tener eso publicitado pero hay mucha gente que no sabe lo que es la ICANN. Si alguien viera el informe sobre lo que está haciendo la ICANN para combatir el uso indebido del DNS, no sabría qué hacer con eso.

Creo que internamente las partes contratadas tienen un trabajo para hacer respecto de publicar lo que hacemos para combatir el uso indebido del DNS. Lo que hacemos, lo que prevemos hacer, y seguir difundiendo a través de grupos como este para tener este tipo de conversaciones con la comunidad. No tengo certeza de que la gente que esté fuera de esta comunidad sepa mucho del hecho de que aparentemente están representados por la gente de esta sala en cuanto al uso de Internet.

GREG SHATAN: Gracias, Reg. Jonathan Zuck.

JONATHAN ZUCK: Estoy en la sala. Muchas gracias. Graeme dijo mucho de lo que había pensado. Muchas cosas interesantes. El enfoque de la fuerza más fuerte es una buena manera. En los últimos años hemos tenido ideas de análisis. No sabíamos la certeza. Había muchos trabajos sobre el tema, de .EU. Hemos tenido este tipo de conversaciones y la mitad se daban en chats y era difícil saber el nivel de realidad que tenían. Lo de las tarjetas de crédito es interesante.

Otra cosa que me viene a la mente tiene que ver con los registros a granel y las de alto volumen y su correlación con el uso indebido. No sé si eso se ha estudiado de manera abierta. Eso es parte de estudio de uso indebido del DNS. Me olvido siempre de la sigla que están usando ahora. Si eso surge de manera concreta y se encuentra una manera de resolverlo sería muy bueno.

Hablamos de estas modificaciones que se implementarían en abril. Corríjanme si me equivoco. Las expectativas es que la gente tiene 18 meses a partir de ese momento para organizarse para cumplir con los requisitos. ¿Hay alguna expectativa de estos malos actores, que tengan tiempo para hacer algo de ahora a abril? ¿Me equivoco?

GREG SHATAN: Reg tiene respuesta.

REG LEVY: No. Preví que iba a empezar a tener quejas sobre el tema.

GREG SHATAN: Tenemos una pregunta remota. Le voy a pedir a la lectora que la lea.

MICHELLE DESMYTER: Tenemos una pregunta de Olivier Crépin-Leblond: “Pregunta para Reg. Por su naturaleza, ¿un nombre de dominio no puede tener un significado o pasar un mensaje o un contenido?”

REG LEVY: Quizá. Hasta donde yo sé no pero es un nombre de dominio y el DNS es el sistema de nombres de dominio.

GREG SHATAN: Aunque tenga contenido o significado no quiere decir que sea juego limpio. Obviamente tenemos temas de mandato o alcance, como dice Reg. Quizá podemos tener un debate bueno y breve pero no es el de hoy, por supuesto. Tenemos suficiente interés en las cosas de las que estamos hablando.

Vamos a ir cerrando. Creo que hemos aprendido mucho sobre el uso indebido del DNS. Hemos aprendido de las modificaciones sobre el DNS y lo que esperamos que traigan aparejado en términos de quejas, cumplimiento y ejecución de la normativa. Los temas de soluciones

potenciales que se pueden llegar a encontrar respecto de los datos de registro. Las inquietudes específicas sobre el tiempo hasta la mitigación y el hecho de que cuanto más tiempo pasa, más problemático puede ser. Finalmente, pero no menos importante, Laureen nos recuerda que al fin y al cabo la meta última normalmente le roban al usuario, lo afectan de alguna manera, ya sea un consumidor individual o una persona jurídica o que recibe algún ataque de ransomware o un intento exitoso de spear phishing o phishing. Hay consecuencias en el mundo real. A menudo es el usuario final el que tiene más para perder. Obviamente nuestro ecosistema y nuestra industria tienen mucho también en riesgo pero esperamos haber alisado un poco las aristas y encontrado maneras de ayudar en esto.

Mucho de esto tiene que ver con la naturaleza fundamental de la Internet o lo que llamamos la paradoja de intermediación desintermediación, porque uno no sabe con quién está tratando pero se puede llegar a los secretos más profundos y viceversa. Ambos pueden estar muy cerca y muy lejos a la vez, de una manera que ningún otro método de comunicación ha logrado nunca. Es sumamente poderoso. Como otras cosas también poderosas, se pueden utilizar para cosas buenas, malas o algo por el medio. No sé si alguien quiere decir algo para cerrar. Ram, está tan callado.

RAM MOHAN: No tengo nada que agregar. Se han dicho cosas muy importantes. No tengo nada para decir. No tengo la necesidad de decir lo que ya se ha dicho.

GREG SHATAN: Lo voy a aprender, Ram, en el futuro. En serio, creo que hemos tenido lindas conversaciones. Muchos puntos interesantes. Es un placer haber tenido este panel. Quisiera agradecer a todos los participantes. Este es un panel de libre albedrío y se ha logrado hablar de temas complejos y no tan claros de manera exitosa. Quisiera agradecerles a todos y decirles que se levanta la sesión.

[FIN DE LA TRANSCRIPCIÓN]