ICANN82 | Foro de la comunidad – ccNSO: sesión del comité permanente sobre el uso indebido del DNS
Miércoles, 12 de marzo de 2025 – 13:15 a 14:30 PST

CLAUDIA RUIZ

Bienvenidos a la sesión del comité permanente sobre uso indebido del DNS de la ccNSO. Junto con Susie Johnson seremos las coordinadoras de participación remota. La sesión será grabada y se rige por los estándares de comportamiento esperado de la ICANN y la política antiacoso de la comunidad de la ICANN. Durante la sesión, las preguntas o comentarios presentados en el chat serán leídos en voz alta si están en el formato que se indica en el chat.

Habrá interpretación para la sesión en inglés, francés y español. Si desean tomar la palabra durante la sesión, levanten la mano en Zoom y cuando digan su nombre los participantes remotos recibirán permiso para hablar en Zoom y los participantes en la sala deberán utilizar el micrófono. Por favor, digan en qué idioma hablarán si no es inglés. Anuncien su nombre y hablen a una velocidad razonable para permitir una interpretación precisa. Ahora le voy a dar la palabra al presidente de la sesión.

NICK WENBAN-SMITH

Bienvenidos. Gracias, Claudia. Ha sido una larga semana de la ICANN. Se aproxima el final. Después del almuerzo reunir la energía pero pedimos que interactúen con los presentadores. La

metodología que hemos elegido para discutir este tema sigue un abordaje no tradicional. Son temas que se han presentado en una encuesta y ha surgido un ganador claro entre las opciones de la reunión ICANN81 en Estambul. El sábado, para darles un adelantado, los dos temas que surgieron al comienzo de la lista para trabajar a futuro son: inteligencia artificial y el rol de la lucha contra el uso indebido del DNS. Ese fue el ganador, ¿no?

Otro tema que tendrá un taller de análisis es el delito financiero en Internet: estafas y el rol de las registraciones maliciosas de nombres de dominio y el uso de ellos para facilitar otros delitos. Así es como llegamos a lo que veremos en las próximas reuniones de la ICANN. Hoy tenemos un formato un poquito diferente, un poquito más de informalidad. Antes de comenzar quiero agradecer al país anfitrión, a .US y a Fernando, quien nos va a contar un poquito lo que pasó en el evento social de anoche.

FERNANDO ESPAÑA Soy Fernando España, de .US. Anoche muchos de ustedes asistieron al evento de networking. Participación que agradecemos. Vimos muchos rostros felices. Sé que la sesión tras el almuerzo es un poquito difícil así que ahí atrás algunos dulces para levantar la energía. Siéntanse en libertad de tomarlos. Sé que es el quinto día de la reunión pero bienvenidos a Seattle. Gracias. Que disfruten.

NICK WENBAN-SMITH

Queremos agradecer a nuestros amigos del registro .US por la recepción anoche. Este tema tan interesante de datos de registración y su intersección entre la recopilación de los datos de registración y la verificación de estos datos de registración, cuál es la intersección que tienen con la prevención y la mitigación del uso indebido del DNS. Un tema muy complicado.

Para mí es un placer recibir dos presentaciones de dos ccTLD distintos. Tenemos a Bob, de .NZ. Gracias, Nigel. Y Kristian, de .SE. Una selección bastante diversa geográficamente de oradores que nos contarán qué están haciendo estos cc con respecto a la recopilación de los datos de registración y el impacto que tienen en las secciones para luchar contra el uso indebido del DNS.

Luego tendremos una visión un poquito más holística. Una de las áreas importantes en los términos de referencia de la ccNSO para el comité permanente del uso indebido del DNS es cómo llegar a las distintas partes de la comunidad de la ICANN. Tenemos el placer de tener aquí a mi buena amiga Reg, de Tucows, registrador global, que tienen una perspectiva distinta de cómo manejarlo. No desde el punto de vista de un ccTLD individual con una política sino con múltiples políticas y también gTLD. Cómo funciona todo esto y si hay mejores maneras de hacer esto colectivamente.

Luego Chris Lewis Evans, quien no está aquí en rol de promoción comercial, nos va a dar su perspectiva como exfuncionario de aplicación de la ley de la agencia de delitos de Reino Unido. Hay un error aquí, en la diapositiva con respecto al horario de la sesión. No

es martes a las 10:30. Por las dudas. Por si piensan que están en alguna simulación kafkiana, en una realidad alternativa del multiverso.

Bob y Kristian comienzan. Si ustedes tienen comentarios o preguntas no está guionado esto. Es interactivo. La idea es interactuar. Como decía en la sesión del sábado hay que hablar. Si yo dije algo que les resultó interesante, planeen intervenir. Sean voluntarios. Estén listos para ofrecerse a hablar. Gracias.

No, había más diapositivas. Estas son diapositivas de introducción. Es un recordatorio. De paso pregunto: ¿Alguno de ustedes aquí es la primera reunión de ICANN a la que asiste? Excelente. Gracias. Bienvenido. Es un grupo muy lindo, muy seguro. Me interesa saber por qué vinieron a esta reunión. Quizá al final me pueden contar.

Los colegas del comité, ¿dónde están? Voy a pedirles que se pongan de pie para mostrarse. Fernando, Bruce, Olga, Chris y David. Muchas gracias a todos. Y Bob. Algo importante a recordar es que no estamos aquí para formular políticas sino para compartir información, mejores prácticas, para aprender de las ideas de los demás y de los errores de los demás. Promover un diálogo abierto y constructivo.

Fundamentalmente queremos promover los ccTLD en el ecosistema. Entendemos que un ccTLD no es más que un TLD. No tiene sentido pasar el uso indebido de un ccTLD a otro ccTLD. No se eliminaría. Es interesante ver qué poco uso indebido existe en la comunidad de los ccTLD en comparación con los TLD. Es

importante que, como ciudadanos, reduzcamos el nivel de uso indebido en toda esta comunidad. Gracias. Siguiente.

Tenemos aquí una lista de los recursos. Hay una librería de uso indebido. Hay una lista de contactos y correos si quieren participar y recibir más mensajes directamente. Hicimos encuestas mundiales de los ccTLD. Una en 2022 y otra en 2024. Los resultados de las encuestas están en los registros y las grabaciones, si les interesan, las pueden consultar. Tenemos sesiones de taller para entender los distintos niveles del DNS a través de distintas herramientas y recursos que se brindan a los ccTLD. Si ustedes no tienen certeza de cuánto nivel de uso indebido tienen, no hay excusa porque hay muchísimos recursos gratuitos disponibles a los ccTLD.

También hablamos de los estándares emergentes por las disposiciones contractuales. La ICANN regula el espacio de los ccTLD respecto de las obligaciones de los registros y registradores. En términos de las denuncias de uso indebido. Entiendo que algunos ccTLD están adoptando disposiciones equivalentes. Siguiente.

En el contexto de entrar a hablar del tema específico de los datos de registración, en la encuesta del 2024, y esta es la introducción del tema de hoy, como ven hay muchas prácticas diferentes para verificar los datos de registración que comprenden ninguna. Algunas personas no hacen nada de verificación. Otras hacen mucho. El tipo de verificación que se haga depende del modelo de

administrador del registro que exista. Está la registración manual, automatizada. Ninguna registración. Solo cuando se recibe un reclamo o algún otro tipo de señal de actividad sospechosa. A veces a la renovación, a veces a la transferencia, a veces antes de la registración, a veces después. Hay varias acciones en el panorama. Siguiente.

Aquí tomemos un momento para entrar a Menti. ¿Están todos conectados o necesitan más tiempo? Me voy a conectar yo. Para tener cierta idea de lo que piensan los presentes. ¿Hasta qué punto están de acuerdo o en desacuerdo con esta afirmación? Que los datos de registración exactos son una herramienta útil para luchar contra el uso indebido del DNS. Estamos viendo cómo suben las respuestas. Tenemos 35. 37, 38, 39, 40, 41. Pueden ver que el número va girando entre 8.5 y 8.2 Roelof, ¿tiene una pregunta? Roelof, si tiene una pregunta.

ROELOF MEIJER: Depende un poquito de cómo se interpreta esta frase porque creo que datos de registración exactos son buenos para prevenir el uso indebido. No estoy seguro de si sirven para luchar contra el uso indebido porque a menudo los actores maliciosos no van a presentar datos exactos.

NICK WENBAN-SMITH: Entiendo a donde apunta. Es interesante porque cuando hacemos estas encuestas en Mentimeter me surge la pregunta: Depende de

con cuánta precisión se lo interprete surgirán distintas respuestas. No es bueno tener preguntas ambiguas.

La idea era general en la palabra combatir o luchar. Vamos a entrar después en esto porque algunos ccTLD utilizan un reclamo contra un nombre de dominio para fines criminales. Usan la verificación de los datos de registración como método para quitar un nombre de dominio del DNS. Lo usan también para herramienta de mitigación. Por eso es una pregunta tan interesante. Hay como un matiz detrás. Eso es parte precisamente de lo que queremos sacar de estas sesiones. Es mucho más complicado de lo que uno puede pensar.

NIGEL ROBERTS

Quería agregar un aspecto más a lo que dijo Roelof, con quien estoy de acuerdo. Nosotros somos unos de esos ccTLD que usted mencionó hace un momento. Le voy a dar la frase completamente distinta. Por eso estoy totalmente en desacuerdo con la pregunta.

Los datos de registración inexactos son una herramienta para luchar con el uso indebido del DNS porque nos han contactado por algunos reclamos reales o imaginarios. Lo primero que hacemos es chequear los datos de registración. Si los datos de registración se ven dudosos, por así decirlo, los ponemos bajo verificación. Si no recibimos la verificación en un periodo razonable, los suspendemos y, por lo general, ahí queda, suspendido.

NICK WENBAN-SMITH

Entiendo la idea. ¿Algún otro comentario antes de entrar en las presentaciones? Pasemos a las presentaciones. Quédense estas ideas. Van a ser temas de nuestra conversación. 8.1 de 10.

BARBARA PEARSE

Soy Barb Pearse, de la Comisión de Nombres de Dominio de Nueva Zelanda. Quiero darles una idea de cómo nosotros manejamos la validación de datos y la verificación de identificación en el ccTLD .NZ. Siguiente, por favor.

Para comenzar con una reseña de lo que dicen nuestras políticas o reglas con respecto a los criterios de elegibilidad. Para registrar un nombre de dominio en .NZ hay que ser una persona física identificable mayor de 18 años o una entidad registrada o constituida lícitamente. No hay un requisito de tener presencia local, lo cual a veces dificulta la identificación de individuos en otras jurisdicciones.

Otro método que usamos es que los datos de registración deben ser exactos completos y estar actualizados. Recolectamos bastante información, incluyendo el nombre del registratario, la dirección, la ciudad, el código postal, el país, etc. Como el caballero dijo, nosotros también podemos suspender o cancelar un nombre de dominio si se determina que los datos son incorrectos o si la identidad no es verificada dentro del tiempo requerido. Siguiente, por favor.

Tenemos dos métodos para hacerlo. Hace poco establecimos una herramienta automática para señalar nombres de dominio maliciosos sospechosos. Asigna un puntaje basado en la información de los datos de registración asignados. En esta tabla se chequea este puntaje de nivel de amenaza y algunos ejemplos podrían ser si hay referencias a gobiernos o servicios financieros como bancos. En ese caso sube el puntaje de amenaza y pasa al proceso de validación de datos. Es un proceso manual ahí, donde enviamos una solicitud al titular de nombre de dominio que tiene que respondernos y confirmar los datos.

El otro método es la muestra reactiva. Es decir, el público, miembros del público nos refieren a nosotros nombres sospechosos y nosotros también ahí iniciamos un proceso de validación. Con respecto a la verificación de la identidad, tenemos un método biométrico de prueba biométrica que es compartido entre múltiples jurisdicciones que requiere que el titular del nombre de dominio se tome una selfie con la fotografía de su identificación para lograr pasar la prueba.

Lo que nosotros vemos a menudo es que el primer paso es una validación de datos. Si se valida pero seguimos pensando en que hay sospecha, lo pasamos por el proceso de verificación de identidad. Lo que solemos ver es que la prueba biométrica no se activa. Si no se realiza el proceso suspendemos el nombre de dominio. Siguiente, por favor.

Lo que hicimos después de la registración, y esto está en la zona, no hay ninguna retención hasta que se completa el proceso de validación. Este es solo un ejemplo de algunos de los pasos durante la muestra de tres meses. En cuanto a la cantidad de proactivos, han sido un 99 % de muestras proactivas suspendidas. 216 de los datos no fueron validados. 7 fueron identificaciones que no eran válidas y 3 verificadas. Es bastante prometedor con respecto a los nombres sospechosos que esperamos poder encontrar.

En cuanto a la muestra reactiva, hubo 51 datos no validados y lo pusimos en la verificación del ID y 3 no fueron verificados. Los que no lo fueron, fueron suspendidos. La muestra reactiva es mucho más baja que la proactiva. En general, la gente se queja de los nombres de dominio que podrían ser un competidor del titular del nombre de dominio o podría tratarse del contenido o del usuario del nombre de dominio. Pareciera adecuado que buena parte de eso no sea verificado porque son titulares legítimos.

NICK WENBAN-SMITH: Si entiendo bien, en las muestra proactivas, estas son las nuevas registraciones que se ven sospechosas y solamente tres, un poco más del 1 %, menos del 99 % son maliciosas aparentemente.

BARBARA PEARSE: El 99 % fueron suspendidas. Tres fueron legítimas.

NICK WENBAN-SMITH En cuanto a la muestra reactiva, aparentemente pasan más porque son nombres de dominio más antiguos.

BARBARA PEARSE O podrían estar comprometidos.

REG LEVY Con las muestras proactivas, 226 fueron en total y 226 fueron verificadas o suspendidas. Con la reactiva, son 97 en total. Pareciera que son más de 70. ¿Qué pasó con las otras 20? Son 97. Okey. Ignórenme. Los totales proactivos están bien. Los suspendidos son 54 más 21. Son 72 dominios.

NICK WENBAN-SMITH Esta es una experiencia muy estresante. Ni siquiera puedo sumar.

REG LEVY Me dijo que estaban bien.

NICK WENBAN-SMITH Yo hice Matemáticas en la Universidad de Cambridge pero eso era más complicado. No creo que 51 más 3 más 21 dé 97. Ese es el punto

REG LEVY ¿Dónde perdimos 20 dominios?

BARBARA PEARSE Probablemente sea un error de cálculo. Los reactivos se verifican y se validan más veces, con más frecuencia.

REG LEVY Yo esperaba que terminaran en la columna verde porque ahí sería 50 y 50 pero si terminan en la columna roja, esto está más cerca del 25 % en realidad. Esos números son números útiles.

BARBARA PEARSE Tenemos 750.000 nombres en nuestro espacio. Es menos del 1 % del total que están en el espacio del uso indebido. Siguiente diapositiva. Nosotros seríamos de la idea de que vemos una fuerte correlación entre los datos no correlacionados que llevan a que hay un indicador de abuso. Esa es la tendencia que vemos en .NZ.

Con respecto a las categorías, la más importante es fake shops y phishing. La que le sigue son las actividades fraudulentas, identidad errónea en los gobiernos e instituciones financieras. Además del compromiso, cuando están comprometidos los nombres de dominio vemos que eso es incorrecto. Lo que suele ocurrir con nuestra agencia de ciberseguridad, lo que ocurre es que nos ayudan a solucionar estos problemas. Esto es todo lo que tenía que decir.

NICK WENBAN-SMITH

Aquí tengo varias preguntas, especialmente respecto a los elementos de política. Es alrededor de un 1 %. Un número pequeño. El procedimiento de verificación es un esfuerzo para los registros en cuanto a costos y es inconveniente en cuanto a la experiencia del usuario, si se trata de un registratario de nombre de dominio. La cuestión entonces es encontrar un equilibrio entre que el TLD sea seguro y que se pueda utilizar comercialmente. Si se trata solamente del 1 %, no deberíamos hacer que la experiencia sea muy pobre para la mayoría de los registratarios legítimos.

BARBARA PEARSE

Es correcto. También tenemos los recursos y la capacidad y lo otro que tenemos que hacer. Tenemos un abordaje específico cuando tomamos la muestra y vamos hacia los más altos.

KRISTIAN ØRMEN

Siguiente diapositiva. Mi nombre es Kristian Ørmen. Soy de la Fundación de Internet de Suecia. Somos el registro de .SE. Aquí unas estadísticas rápidas. Tenemos 105 registradores. Estamos abiertos para registraciones de todos los lugares del mundo. Tenemos unos requisitos bastante estrictos. Son requisitos donde el registratario tiene que verificar el registro. Tratamos de todos modos de ser razonables. Tenemos casi 1.7 millones de dominios en total y un modelo de precios donde tenemos distintos tipos de incentivos para los registradores y así también es como tenemos nuestro precio promedio de registración. Uno de los incentivos es que damos un descuento a los registradores que utilizan el eID para

verificar a los registratarios. Eso es bueno para algunos pero no para todos.

La pregunta primero es si la verificación del registratarios va a solucionar el tema del uso indebido y la respuesta es absolutamente no. Los datos imprecisos son una muy buena herramienta para cerrar los sitios de uso indebido. Estoy de acuerdo pero sin importar de qué manera hacemos la verificación y cuántos dominios se verifican. Esto nunca va a solucionar el problema del uso indebido.

Los atacantes van a poder circunvalar las reglas. Van a poder saber qué ocurre con la verificación cuando uno vende un dominio por un euro. En nuestro caso es un poco más caro pero tenemos que ser razonables. Tenemos que poder considerar el uso indebido cuando sucede sin importar si es preciso o no, si es correcto o no. De todos modos, tenemos que enfrentarlo.

Por supuesto que es útil dar datos de registratario precisos cuando los tenemos. A mí no me gusta mucho cuando nos contactan y nos dicen: “Este es el dominio de El Pato Donald”. Esta no es una buena sensación. La alternativa muchas veces es que digamos que esto está registrado en la empresa A-B pero esos datos también estaban equivocados porque habían sido tomados directamente de la base de datos de la empresa cuando se registró. A pesar de que son buenos datos, siguen siendo inválidos porque no son los datos del registrador.

También, por supuesto, en el caso de sitios web que han sido jaqueados o utilizados inadecuadamente, es bueno tener buenos datos para contactar al registratario. Otra cuestión importante para mí, en mi registro, es que queremos datos correctos en los dominios porque queremos garantizar que los registratarios no pierdan esos dominios.

Queremos poder verificar a un registratario cuando viene y dice: "He perdido mi dominio con este registro y este registro no me ayuda". Cuando miramos, es El Pato Donald. Le decimos: "No, este no es su dominio". Si tu nombre es Anders Andersen, tendría que figurar eso en el registro. Ahí podemos verificar que ese dominio te pertenece a ti. Eso es lo más importante para mí. Es la razón por la cual creo que tenemos que corregir los datos del registratario.

Como dije antes, tratamos de ser razonables con respecto a nuestros requisitos para la verificación. Cuando un registrador me pregunta cuánto tengo que verificar en general respondo que al menos tenemos que esperar no ver datos falsos en lo que se refiere al uso indebido. Si usted está registrado en Suecia y tiene muchos clientes suecos con datos abiertos, eso se puede utilizar para ver si la empresa existe, si el nombre es correcto, etc. y este es un método muy bueno de verificación. Incluso si tenemos que encontrar dónde está la firma y le pedimos que se loguee, quizá esto sea demasiado. Por eso, eso no se lo pedimos a los registratarios. Hemos implementado un nuevo sistema donde pedimos un poco más.

Para los nuevos dominio hay un descuento al utilizar la EID, como dije antes. También tenemos verificación predelegación donde consideramos la registración y si ese testeo falla vamos a enviar un error al registrador y le vamos a pedir que reverifique al registratario.

Ahí somos un poco más estrictos y decimos: “Hay que hacer una verdadera verificación”. Hemos diseñado entonces ese sistema de manera que lo más importante sea que se pueda extender el sistema después sin introducir ningún cambio para los registradores. Por eso lo hicimos de esta manera. Si hay un error, hay que reverificar el registratario pero con nuestras verificaciones podemos extender el tiempo además de usar los datos externos. Utilizar inteligencia artificial para ver si hay un dominio equivocado. También podemos ir cambiándolo con el tiempo pero los registradores van a seguir teniendo la misma experiencia y esto es importante para nosotros.

En este momento hay un nuevo sistema y lo hemos hecho intencionalmente. Hemos sido muy leves. Hemos dejado unos 100 dominios en dos meses. Tenemos verificaciones que no hemos activado todavía. Tanto nosotros como los registradores nos tenemos que acostumbrar a este nuevo cambio. Esta es una de las razones por las cuales está funcionando así.

NICK WENBAN-SMITH ¿Cuando empezaron con la solución de eID?

KRISTIAN ØRMEN

El eID es un incentivo, un descuento que comenzamos en enero de 2023. Ahora tenemos los dos registradores más importantes utilizándolo y algunos de los más pequeños también. Estamos en alrededor del 40 % de nuevas registraciones que se validan con eID. Son alrededor de dos dólares y medio, 25 coronas, y esto ayuda a pagar el costo del sistema. Para algunos registradores, especialmente para los más grandes, es muy interesante porque se ahorran mucho dinero.

NICK WENBAN-SMITH

Tengo algunas preguntas. Creo que Luc va primero y luego veo por aquí a Bruce y a Reg.

LUC SEUFER

Luc, de EuroDNS. Es una pregunta creo que para Barbara. No entendí muy bien el nombre. Vi el término fake shop muchísimo esta semana en distintas presentaciones. Quiero saber qué significa. ¿Es una persona que suplanta la identidad de un usuario? ¿Es como phishing? ¿Es una empresa que vende mercaderías falsas o se trata de una cuestión de protección de propiedad intelectual o qué es?

BARBARA PEARSE

Desde nuestra perspectiva, tiene más que ver con la suplantación. Alguien con el nombre cambiado en el nombre de dominio que no parecía ser esa organización. Podría ser phishing pero nosotros no

realizamos un análisis para determinar si eso es así o no. Simplemente hacemos el proceso de validación de datos y en la mayor parte de los casos hay una suspensión.

LUC SEUFER ¿No el uso indebido del DNS según la definición de ICANN?

BRUCE TONKIN En cuanto a fake shop. Otra definición de fake shop es cuando uno pide algo y no se lo envían. Parece un buen negocio. Tiene servicios y bienes. A uno le cobran en la tarjeta de crédito pero no recibe lo que compró. No es como phishing porque no es necesariamente que se vea como una marca en particular. Es una empresa donde uno puede comprar un negocio, donde uno puede comprar.

NICK WENBAN-SMITH Hablamos de esto el sábado. Dijimos que tendríamos que dedicar más tiempo a la definición de alguno de los términos. Qué es uso indebido, qué es phishing. Lo que vemos es que se puede dedicar mucho tiempo a las definiciones y qué es lo que es un delito, qué es phishing, qué es propiedad intelectual, violación de la propiedad intelectual. Hay muchas capas pero creo que se trata de actividades criminales, fundamentalmente, y que la mayor parte de los ccTLD tienen políticas y procesos establecidos para quitarlos de su TLD. Es interesante lo que puede ser fake shop.

BRUCE TONKIN Una pregunta para Kristian. Cuando usted habla del eID, ¿a los registradores les cobran por hacer esos chequeos o es gratuito?

KRISTIAN ØRMEN Estamos abiertos a que el registrador pueda elegir la solución eID que quiere. Tenemos algunos requisitos estandarizados. En Suecia hay uno muy grande que se llama Bank ID. Es una transacción que es mucho más barata que nuestros incentivos y es muy bueno pero si hay registratarios de otros países, eso no funcionaría. Habría que encontrar otro proveedor de eID de ambos países.

NICK WENBAN-SMITH Muy interesante. ¿Es claro en el caso de RDAP o de WHOIS o de otros tipos de registros que los dominios han sido verificados y que algo es confiable y seguro?

KRISTIAN ØRMEN En este momento no lo mostramos en el WHOIS. Lo utilizamos como incentivo.

NICK WENBAN-SMITH Chris.

CHRIS LEWIS-EVANS Kristian, ¿usted dice que esto está funcionando desde hace dos años, el eID? ¿Tiene algún dato en cuanto al nivel de uso indebido

con aquellos que se registraron con este mecanismo versus los que no se verificaron con el eID?

KRISTIAN ØRMEN

No tengo esos datos actualmente. El año pasado estábamos en el 20 %. Ahora en un 40 % del volumen que se va ampliando pero la mayor parte del uso indebido que vemos es de los registradores que no utilizan los incentivos de eID. Creo que no sería un gran cambio pero no hemos profundizado aún en eso.

NICK WENBAN-SMITH

¿Les van a ajustar las clavijas a los registradores? ¿Van a empezar a utilizar la barra del cumplimiento o van a dejar el incentivo?

KRISTIAN ØRMEN

Para eID mantenemos el incentivo. Cuando hablamos de uso indebido tenemos unos requisitos bastante leves. En la actualidad, en cuanto a los registradores en la parte de la verificación y en lo que se refiere a todos los dominios, el año pasado, no sé si lo puse en la diapositiva pero podemos ir a esa próxima y verlo.

Hemos incluido un requisito en nuestro contrato para los registradores de que si conocen que existen datos incorrectos en la registración tienen que actuar, tienen que contactar al cliente. Si no se cambia dentro de un periodo razonable, deben desactivar el dominio.

Esta es una de las cuestiones que hemos agregado para los registradores, que es una gran carga considerando que hay muchos dominios anteriores con datos incorrectos pero también es bueno en el sentido de que si uno ve un dominio con uso indebido, todos nosotros sabemos que en general tiene datos incorrectos. No siempre pero en la mayor parte de los casos.

REG LEVY: Una pregunta sobre los incentivos al eID. Pareciera ser sencillo que es fácil hacer esta verificación pero no lo es tanto en el Reino Unido. ¿Podría un registrador tener precios preferidos para los dominios que sí brindan verificación a través de eID pero menos para los que no lo hacen?

KRISTIAN ØRMEN: Por dominio. A ver si entiendo. Que el registrador demuestre que utiliza el eID o no. En el caso de que lo use, nosotros tenemos un pool de registradores que hacen eso y estamos probando.

PIERRE BONIS: Muchas gracias. Gracias por la presentación. Quiero saber, cuando ustedes verifican un nombre de dominio nuevo y deciden no activarlo, ¿se lo cobran al registrador?

KRISTIAN ØRMEN: El dominio quedará registrado pero aparecerá un error con un registro de reverificar y el nombre estará en el registro hasta que se

produzca su fecha de vencimiento. Estará en un estado de hold durante un año. No vemos razón para suprimirlo porque facturamos al registrador y tiene todo el tiempo que quiera para arreglarlo. Si no lo hace, no se activa.

PIERRE BONIS Si el registrador decide suprimirlo, porque se ha dado cuenta de que los datos están corruptos o no son buenos, ¿le cobran al registrador o les dan un periodo de gracia?

KRISTIAN ØRMEN Usualmente no cobramos. A veces si el registrador ha sido jaqueado o si la cuenta del registratario tiene mil nombres registrados, le decimos al registrador si puede presentar un informe de incidente con un comentario de cómo puede prevenir esto para el futuro y podemos hacer una nota de crédito pero normalmente no damos crédito a nombres de dominio que ya están registrados.

ROELOF MEIJER Gracias. ¿Tienen alguna información sobre el impacto de nombres registrados maliciosamente y aquellos que tienen verificación eID?

KRISTIAN ØRMEN No. Creo que no tenemos. Creo que no existen los impactos. Tendríamos que hacer un análisis más profundo de estas cifras. Por ahora es un programa voluntario. Todavía es posible registrar sin

el eID. Creo que es una buena curva hasta el 40 %. Tenemos más registradores que se centran en la verificación. Podemos tener buenos datos con estas registraciones pero no creo que esto tenga ningún efecto todavía.

NICK WENBAN-SMITH ¿Esta iniciativa está conectada de alguna manera con las obligaciones de la NIS2?

KRISTIAN ØRMEN Sí y no. Desde que comenzamos hace mucho tiempo sabíamos que iba a ver requisitos de verificación con NIS2 y queríamos comenzar a trabajar temprano pero no queríamos registros sumamente exigentes para los registradores. Tampoco conocíamos el texto exacto de la NIS2 y queríamos comenzar con este incentivo para ver que la gente comenzara a trabajar y también queríamos que los registradores hicieran verificación y que mostraran que era posible.

Si surge un requerimiento por ejemplo de la Unión Europea, en caso de surgir un requerimiento, que no tuviéramos que poner un flujo de orden nuevo. Normalmente esto requiere hablar directamente con el registratario. En este caso, es la parte del negocio del registrador.

NICK WENBAN-SMITH ¿En Suecia hay una célula de identidad?

KRISTIAN ØRMEN En la Unión Europea normalmente hay. Nosotros somos uno de los pocos países que no lo tiene pero esa es otra historia.

NICK WENBAN-SMITH En el Reino Unido tenemos tarjetas de identificación nacionales pero no sé si va a entrar en vigencia alguna modificación.

KRISTIAN ØRMEN Quería explicar un poco mejor lo de la diapositiva. Desde el 1 de mayo vamos a activar un nuevo sistema para poder trabajar en volumen con todos los dominios. Lo que podemos hacer es lo siguiente. Si encontramos un dominio que tiene datos extraños o raros podemos poner esos dominios en el sistema y el registrador recibe un mensaje con la fecha en que tiene que reverificar el dominio.

Vamos a dar inicialmente 60 días, a menos que pase otra cosa. Como ejemplo tenemos 12.000 dominios que podemos ver en el registrador de una compañía que ya no existe. Dominios así los vamos a incorporar. Si vemos dominios en los feeds de uso indebido con datos extraños, le damos menos días al registrador. Por ejemplo, cinco. Dependiendo del caso. Es flexible. También sigue el mismo camino que en este sistema de nuevos dominios. Creo que, si no me equivoco, esta era mi última diapositiva. Sí.

NICK WENBAN-SMITH Muy interesante. ¿Alguna otra pregunta? ¿.SE es un registrador? ¿Qué piensa de todas estas nuevas reglas? ¿Les gustan los incentivos financieros?

REG LEVY Tengo un equipo que se ocupa de las reclamaciones casi exclusivamente, de reclamaciones de gTLD. Porque hay tantos ccTLD que manejamos que nosotros tenemos un equipo aparte de ccTLD para ocuparse de eso. Si es uso indebido del DNS, viene a nosotros, pero si hay que suspenderlo o alguna otra cosa, ahí va a otro equipo. Los ccTLD son muy confusos.

NICK WENBAN-SMITH Sí, sí. Son dos ejemplos muy distintos ya. Por eso el desafío de tener estos estándares diferentes entre los distintos ccTLD. Eso constituye un riesgo. Permite que los actores maliciosos exploren los vacíos en los distintos lugares. En Dinamarca, Suecia, lo que pasa con la identificación, por ejemplo.

Volviendo al punto original, que es que la vasta mayoría de las registraciones, especialmente en los ccTLD son totalmente legítimas. Aun cuando los datos no pueden ser tan buenos en lo fundamental son registraciones legítimas. Es un costo inconveniente que se impone a todos y no tiene una lógica industrial, me parece.

REG LEVY

Nosotros pensamos que la mayoría de las registraciones son legítimas más allá de cuáles sean los datos de registración pero no ha sido nuestra experiencia que se nos utilice como objetivo porque tenemos tantos ccTLD. La mayoría no sabe ni que existimos porque nosotros somos un registrador mayorista. Nuestros clientes principales son suecos. Nuestros clientes en .DE es un puñado de revendedores alemanes. Todos son excepciones. Lo que vemos es que Tucows no es objetivo de uso indebido porque no hay tantos TLD.

NICK WENBAN-SMITH

¿Cuál es su opinión? Usted piensa que existe utilidad en los datos de registración, ya sea en el punto de registración para prevenir las registraciones maliciosas o en respuesta a reclamaciones, a phishing, a botnets, a feeds. ¿Seguir el proceso de verificación de los datos para sacar un nombre de dominio del DNS? ¿Ustedes están por encima del promedio o por debajo del promedio o es una molestia total?

REG LEVY

Yo estaba por debajo del 8.1 porque no veo una correlación entre lo que se llama la verificación, y eso después lo explico, y el uso indebido del DNS u otros tipos de uso indebido. Esto puede percibirse también con respecto, y aquí no me la voy a agarrar con ningún ccTLD, sino con .EDU. .EDU tiene requisitos sumamente estrictos para cómo conseguir un .EDU. Hay que ser una entidad. No es cualquiera. Tiene elevados niveles de uso indebido, sí.

Muchísimo a través de dominios comprometidos porque .EDU permite a los estudiantes, permite mucho acceso abierto a dominios y subdominios, URL y ese tipo de cosas.

No siempre parece existir una relación entre los datos exactos y el uso indebido. Digo datos exactos, por así llamarlos, porque la definición de exactitud es distinta. Kristian tiene un ID electrónico y Barb tiene una prueba biométrica. Ambos son totalmente diferentes. Ambos van a decir que son verificables y exactos pero cada TLD determina qué es de manera diferente. Cuando uno dice: "Los datos exactos son útiles para luchar contra el uso indebido, no sé, en primer lugar, qué significa exactos porque hay diferencias". En segundo lugar, yo no veo una correlación ni en los ccTLD ni en los TLD entre datos exactos, si es que decidimos qué es, y la presencia o ausencia de uso indebido del DNS.

NICK WENBAN-SMITH Interesante reflexión. Muchos aquí pasamos mucho tiempo y mucho trabajo asegurándonos de que los datos subyacentes sean exactos porque pensamos que, como registro, tener datos exactos y limpios son como un principio fundamental importante.

KRISTIAN ØRMEN Quiero agregar que nosotros tenemos muchos más datos inexactos que uso indebido. No se puede decir que una registración inexacta es una registración abusiva. Son dos cosas completamente diferentes.

NICK WENBAN-SMITH Exacto. Muchos ccTLD en el Reino Unido, si alguien se queja de un nombre de dominio o por phishing o recibe una alerta, lo primero que hacemos es ver los datos de registración y pensar que es la solución rápida, y lleva tiempo y esfuerzo investigar estas cosas. Ahí se ve rápidamente que los datos de registración, si están muy mal, es una clave inmediata.

CHRIS LEWIS-EVANS Voy a volver al comienzo. Soy Chris Lewis Evans. La pregunta era cuán útiles son los datos de registración exactos para luchar contra el uso indebido. ¿Qué es luchar? ¿Qué es combatir? Chris dijo útil para la policía. Mi visión de lucha del uso indebido es retirar el nombre del sistema en línea, para proteger a la gente. Los datos inexactos es una buena manera de decir que probablemente esto sea algo que se usa para información falsa. Aparece la policía. Se saca y muy bien. La gente está protegida. La policía luchó contra el uso indebido.

En muchos casos con los ccTLD hay largos periodos de registración de nombres de dominio y lo que vemos es que cada vez más nombres de dominio tienen siete años o más. Hablando del caso de .EDU, ahí hay más compromiso. Nosotros no queremos suspenderlos. Queremos arrestar a la persona que ha comprometido pero eso lleva mucho tiempo. Los datos inexactos no nos sirven para restar. Lo que sí nos sirve para restar es respaldar a la persona que se ha visto comprometida. No estoy

yendo en contra de los cc pero cómo nosotros, los organismos de protección de la ley, protegemos a alguien que no podemos contactar.

Esa persona puede estar detrás de un CDN. Tenemos que ir al CDN. La persona puede estar haciendo el alojamiento ella directamente. Si uno tiene propio alojamiento, seguramente tendrá cierta seguridad pero no es muy buena. Los datos exactos son muy útiles desde la perspectiva policial para luchar contra el uso indebido porque podemos contactar a la persona. Solo sacar el contenido es una parte importante de la lucha contra el ciberdelito, el delito en línea, como se lo quiera llamar. Creo que es probablemente la parte más importante de por qué los datos exactos son útiles. Recomendaría a los cc que sigan haciéndolo.

Del otro lado, por otra parte, brinda una barrera o un punto de fricción con las registraciones. En general, los criminales son haraganes. Van a donde es barato, donde consiguen un impacto entre la gente. Si piden un ID electrónico o prueba biométrica, se van a otra parte. Si todos tienen problemas de registración, igual lo van a hacer porque quieren ganar dinero, es su negocio.

¿Es la panacea luchar contra todo el uso indebido? No. Claramente. El uso indebido va a seguir. Ahora, ¿esta fricción ayuda? Sí. Para mí, para luchar contra el ciberdelito habría que permitir a la policía y a otros organismos, permitir contactar a la gente y poder bajar el dominio.

REG LEVY

Desde mi punto de vista, nosotros nos centramos en la capacidad de contactar. Contactabilidad. Si podemos contactar al cliente porque mucho del uso indebido se refiere a situaciones de compromiso y si nosotros podemos hacer una referencia derivarlo está bien. Dirección de correo electrónico, en la mayoría de los casos son válidas. La idea es poder contactar pero a mí me parece que a veces con este uso excesivo de Internet no se pide identificación cuando la gente compra pero en algunas áreas, si hay que expresar esa línea, se exige algún tipo de identificación. No solo en el espacio de los ccTLD. Algunos sitios de redes sociales requieren cosas similares. Esto a mí me preocupa.

NICK WENBAN-SMITH

¿Hay alguna consulta en la sala de Zoom?

BRUCE TONKIN

Quería hacer un comentario sobre lo que dijo Reg. El plazo de las nuevas registraciones, algunos días o un mes, estos datos de registración relacionados con los dominios comprometidos. Vemos en promedio nombres que están hasta siete años. No sé si hay alguna solución de gestión de contenidos. Es una característica común que vemos. A menudo los datos de registración están desactualizados. Esa sería la expresión correcta. Desactualizados y no inexactos.

Lo que los registradores suelen hacer es que tienen información de facturación desactualizada. En general una tarjeta de crédito. Si hay una renovación, sacan la tarjeta del archivo y esa es la información que tiene el registrador. Es otro desafío que los nombres comprometidos. Normalmente dependemos de los registradores que contraten al registratario para que los contacten con otros datos que pueden tener.

NICK WENBAN-SMITH

Como dijo Chris, es un disruptor. Son herramientas para la disrupción. La existencia del lavado del dinero o del antilavado de dinero a través de los bancos no evita que haya lavado de dinero. Eso no quiere decir que las instituciones bancarias no tengan que estar acostumbradas a lavar dinero. Kristian, Pierre y Reg.

KRISTIAN ØRMEN

Para continuar centrándonos en la cuestión de la posibilidad de contactar, la contactabilidad. Nos pareció que teníamos que ser mucho más estrictos pero NIS2 surgió con unas recomendaciones no vinculantes y el foco principal, y esto es lo que me parece interesante, es email y número de teléfono. Luego hay algunas otras definiciones que no sé muy bien cómo interpretar todavía pero dicen que para los dominios con riesgo medio y alto recomendamos verificar el nombre del registratario también.

Cómo leo esto entonces. Básicamente la verificación del email y el número de teléfono es lo más importante, y esperamos que esto se

haga en todas las registraciones y también esperamos que algunas registraciones hagan una verificación más profunda. No soy abogado pero me parece interesante que haya muchos menos requisitos de lo que yo esperaría. La posibilidad de contactar definitivamente es lo más importante.

NICK WENBAN-SMITH

En mi experiencia al tratar con reguladores, como abogado, si uno tiene mucho uso indebido esto se toma como evidencia y no se hace la verificación. Es decir, un ccTLD tiene que estar limpio y hay que tener una buena acción defensora para los reguladores, no solamente en beneficio de las personas.

PIERRE BONIS

Quiero agregar dos cosas. La importancia de la contactabilidad cuando hablamos de los nombres de dominio comprometidos, lo importante es que se pueda contactar al registratario, no que sepan que es Pierre Dupont. Esto es mucho más fácil de hacer para un registro. Garantizar que el registratario responda y también asegurarse de que el registratario es quien dice que es.

En segundo lugar, me hago eco de lo que ha dicho Kristian. Cuando utilizamos la verificación de los datos para luchar contra el uso indebido, y es lo que hacemos en .FR, esta es la herramienta principal, más del 99 % de las verificaciones que lanzamos cuando sabemos que hay un uso indebido nos demuestran que los datos están equivocados, que no son buenos datos. Por el contrario, los

datos no actualizados, los datos inexactos no llevan a ningún tipo de uso indebido. Esta equivalencia entre datos limpios y no uso indebido no es muy convincente a fin de cuentas.

NICK WENBAN-SMITH Cuando AFNIC contacta al registratario para hacer la verificación o mirar los informes, ¿el registratario sabe quién es AFNIC? ¿Cómo lo convence uno de que no es un email de phishing en sí?

PIERRE BONIS Es una buena pregunta porque a veces el registratario dice: "No sé quién es usted". Quizá es un scammer. Esa información o ese pedido lo enviamos al registrador y al registratario a la vez. Es decir, al menos si no confía en nosotros, por lo menos tiene que confiar en el registratario.

NICK WENBAN-SMITH A veces el registrador no es la misma persona que el registratario contactó. Podría ser un revendedor o una empresa que utiliza al registrador. A veces puede ser muy confuso.

PIERRE BONIS Por eso tenemos en nuestro sistema dos capas después de cinco días, que es bastante breve ese plazo. Lo mantenemos y después de 30 días lo borramos. Cuando uno suspende va a su email y trata de saber por qué y contacta al revendedor o al registrador y trata

de entender por qué el nombre de dominio no funciona. Si damos la respuesta en minutos uno vuelve a estar online otra vez.

NICK WENBAN-SMITH Mi duda al hablar de los datos de registración como una herramienta para combatir el uso indebido es que si uno es un actor amenazante es lo suficientemente inteligente como para hacer una registración mala y crear una desconfianza en horas y minutos antes de que este proceso entre en vigencia. La pregunta de si es lo suficientemente bueno es interesante y es útil pero no es completo como solución. Primero Kristian.

KRISTIAN ØRMEN Una breve respuesta. Nosotros también utilizamos estas verificaciones. Lo hacemos con los registradores también. Hay que tener en cuenta que también hay que incluir al registratario. Si le damos un plazo de 24 horas, por ejemplo, eso es muy poco. Hay que darle un tiempo razonable para reaccionar.

Claro que también hay que ver cuán malo es lo que estamos analizando y establecer un tiempo en función de eso pero hay que ser razonable y hay que poder dar pruebas como, por ejemplo, después de la suspensión pueden lograr que el dominio funcione otra vez. No dar un poder excesivo porque nosotros no somos la policía. Nosotros estamos creando políticas que ayudan a la sociedad que trabaja en los dominios de Internet pero la policía tiene que ser la policía.

NICK WENBAN-SMITH Primero Luc. Después Irina.

LUC SEUFER Esa es la ley en lo que se refiere a los datos imprecisos. Yo no estoy de acuerdo con Chris. Los delincuentes no siempre son tan holgazanes. Si uno quiere algo específico, lo va a lograr. Para dar un poco de color, estamos vendiendo el .CU de Cuba. Se requiere presencia local y lo estamos vendiendo a 1.200 dólares por año. A veces, de todos modos, tenemos uso indebido. No hay una solución mágica.

NICK WENBAN-SMITH Irina.

IRINA DANELIA Soy Irina, de .RU. Estamos hablando del segundo nivel de registraciones. Tomemos esto como un ejemplo. Nosotros tenemos procesos y procedimientos para suspender nombres de dominio pero en este momento podemos decir que gran parte del uso indebido del DNS es tratado en el tercer o cuarto o quinto nivel. A mí me interesaría saber qué piensan ustedes sobre cómo tenemos que enfrentar esto. ¿Debe haber una penalidad para los titulares de segundo nivel o hay alguna otra idea?

NICK WENBAN-SMITH Reg se ofrece para hablar de esto.

REG LEVY No me voy a girar para contestarle. Me disculpo por ello. Sí, nosotros vamos a considerar al titular de dominio de segundo nivel porque cuando esto ocurre en el tercer o cuarto o quinto nivel, esto se debe a que el dominio de segundo nivel fue registrado maliciosamente y lo podemos suspender. Eso está muy bien. Significa que el segundo nivel ha sido comprometido porque el registro de DNS comienza en el segundo nivel.

La persona que tiene acceso al dominio de segundo nivel va a tener acceso también al tercero y al cuarto. Utiliza el término dominio de segundo nivel para decir que en el tercer nivel, en el .CO.UK, porque estamos vendiendo .CO.UK como el primer nivel. Por eso técnicamente este es el segundo.

NICK WENBAN-SMITH Vamos a repetir la pregunta. Muy rápidamente. Vamos a repetir la encuesta.

KRISTIAN ØRMEN Tenemos otro jugador en la industria que vende .COM.SE. Ahí recibimos muchos informes de uso indebido. No podemos hacer nada más que decirle al registro .COM.SE que trate estas quejas, estos reclamos. Si cerramos el .COM.SE también vamos a cerrar verdaderas empresas. Un ejemplo reciente es la cadena Five Guys, que no podían registrar fiveguys.com y registraron

fiveguys.com.se. Va a haber muchos dominios como este que son problemáticos pero puede haber dominios buenos también. No podemos suspender toda la zona.

NICK WENBAN-SMITH Tiene que haber un elemento de proporcionalidad. Creo que podemos hacer la encuesta después de esto.

CHRIS LEWIS-EVANS En cuanto a AFNIC, cuando uno envía un email puede ser que no crean en quién es uno o no sepan quién es uno. Tener múltiples puntos de contactabilidad es importante, especialmente cuando hay un compromiso. Si está comprometida la dirección de email, no se puede garantizar la contactabilidad a través de un mecanismo. Es decir, hay que tener datos exactos en todos los puntos de contacto. Esto es muy importante. No solamente para un único email. Esto se hace incluso más importante cuando está vinculado a un dominio. Si uno lo suspender no se puede contactar con esa dirección de email.

NICK WENBAN-SMITH Eso lo vi con dominios que yo suspendí. Ponía los ojos en blanco porque veía que había un contacto de email donde el registratario es el mismo que acabamos de suspender y el email no va a funcionar. No es muy inteligente. Vamos a repetir.

No me puedo acordar de cuánto tuvimos la primera vez. 41 participantes. ¿No es interesante la vida? Esto no es lo que

esperaba. Tuvimos un debate muy largo con expertos sobre la importancia de los datos de registración y el resultado es que parece que es menos importante. ¿Lo interpreté bien o no?

KRISTIAN ØRMEN Los datos de registratarios son importantes para muchas personas pero, como decía en mis diapositivas, no va a resolver el problema del uso indebido. Creo que el hecho de que el puntaje sea bajo está diciéndolo también en voz alta.

NICK WENBAN-SMITH No es mucho más bajo. Es un poco más bajo. Uno de mis libros favoritos es sobre la evidencia médica en ensayos clínicos. El título es: “Yo creo que usted lo va a encontrar más complicado que esto”. Los datos de registración, las definiciones, los problemas, la contactabilidad, la complejidad del ecosistema, las distintas reglas, los distintos espacios geográficos, la inteligencia de los actores, el ingenio de los que quieren ganar dinero a través de medios criminales, todo esto hace que sea mucho más complicado de lo que se ve a primera vista.

Este es el final de esta sesión oficial. Quiero agradecer a todos. Ha sido muy buena la participación. Si hay alguien que quisiera decir algo más me pueden encontrar a mí muy fácilmente. La sesión de los recién llegados también ha sido muy buena. Les agradezco a todos por haber estado aquí. Gracias a los excelentes panelistas.

[FIN DE LA TRANSCRIPCIÓN]