ICANN73 | Foro virtual de la comunidad – Sesión plenaria: evolución de la conversación sobre el uso indebido del DNS
Miércoles, 9 de marzo de 2022 – 10:30 a 12:00 AST

BRENDA BREWER: Hola y bienvenidos a esta sesión plenaria de la reunión ICANN73, que es la evolución de la conversación sobre el uso indebido del DNS. Mi nombre es Brenda Brewer y coordinaré la participación remota, por favor tengan en cuenta que esta sesión está siendo grabada y sigue los estándares de comportamiento esperado de la ICANN, a fin de garantizar la transparencia en la participación dentro del modelo de múltiples partes interesadas de la ICANN.

Les pedimos que ingresen a las sesiones de Zoom utilizando el nombre completo, por ejemplo, primer nombre y apellido, podrían ser eliminados de la sesión si no se registran con su nombre completo. La interpretación para esta sesión incluya árabe, chino, francés, ruso y español. Hagan clic en el ícono de interpretación en la barra de herramientas de Zoom para seleccionar el idioma de preferencia.

Durante esta sesión las preguntas o comentarios enviados al chat solamente se leerán en voz alta si se encuentran en el formato adecuado, tal como indicaré en el chat, leeré las preguntas y comentarios en voz alta cuando sea el momento durante esta sesión.

Durante esta parte del debate de la comunidad si desean tomar la palabra, por favor hagan clic en levantar la mano en la barra de herramientas de Zoom, antes de tomar la palabra por favor silencien sus dispositivos y notificaciones, también asegúrense de haber seleccionado el idioma de preferencia al escuchar.

Les pedimos que hablen a una velocidad razonable y de manera clara para la interpretación. Una vez que el facilitador de la sesión diga su nombre, les pedimos que por favor activen su micrófono y que digan su nombre para el registro. Para ver la transcripción en tiempo real hagan clic en el ícono "subtítulos" oculto en la barra de herramienta de Zoom y ahora le damos la bienvenida al moderador de esta sesión, Graeme Bunton, adelante por favor.

GRAEME BUNTON: Muchas gracias, Brenda. Buenos días, buenas tardes y buenas noches a todos, gracias por unirse a esta sesión plenaria, que es la evolución de la conversación sobre el uso indebido del DNS, las registraciones maliciosas y nombres de dominios comprometidos. Yo soy Graeme Bunton, soy miembro del instituto del DNS y me quiero disculpar por la falta de presentación, pero hoy tenemos un muy buen panel y un tema muy complejo, así que, les pido que me tengan paciencia.

Nuestro primer presentador, Maciej, nos va a dar una introducción más concreta al tema y quiero asegurarme de que a los fines de la presentación todos estemos en la misma página, así que, les voy a explicar de qué vamos a hablar hoy. De manera simple, nuestra sesión

el día de hoy va a versar sobre el proceso de mitigación para los dominios que han sido creados para causar daños y para aquellos dominios o sitios webs que han sido hackeados o comprometidos y que se utilizan para causar daño.

En un caso lo que se trata es de crear daño con un nombre de dominio y en el otro caso no, pero tenemos que entender cuál es la complejidad que esto plantea para nuestro ecosistema, así que, antes de adentrarnos en la sustancia de esta presentación, quiero hablar del alcance de esta sesión y darles unas pautas para estructurar estar conversación.

Brenda, si me permite quisiera pasar a la siguiente diapositiva. Los objetivos de esta plenaria, eso es lo que vamos a tratar de lograr el día de hoy en este breve tiempo que tenemos, queremos desarrollar una comprensión de la comunidad sobre por qué esta distinción es importante entre un nombre de dominio malicioso y comprometido, también queremos ver cómo hacer esta distinción. No vamos a entrar demasiado en los detalles técnicos.

Luego queremos también ahondar en el entendimiento de la comunidad de qué es lo que se puede hacer en cualquiera de los dos escenarios y, finalmente, queremos hablar de las posibles actividades, qué podemos hacer sobre este problema, quién debería tomar acción y cuál es el rol de la comunidad. Pasemos por favor al alcance, este es importante.

Yo estuve ocupado en las cuestiones de la ICANN durante un tiempo, estuve participando en varias plenarias y creo que hay una relación en cuanto a la especificidad del tópico y cuánto nos llevaremos de esta sesión, así que, yo quiero que hoy aquí todos seamos bastantes acotados en nuestro alcance el día de hoy.

Hay algunas suposiciones a tener en cuenta al momento de llevar adelante el debate, vamos a hablar aquí de un registrador o registro que ha recibido un informe sobre uso indebido, cómo ese informe se recibió y si está o no en debate. Vamos a suponer que el uso indebido ha sido verificado, no vamos a debatir si está sucediendo o no, la verificación está fuera del alcance.

Primeramente, nos vamos a focalizar si es phishing o no, no vamos a definir uso indebido del DNS, probablemente hay varias definiciones de uso indebido del DNS, pero no estamos aquí hoy para debatir esa definición quiero ser muy claro aquí, no vamos a entablar un debate sobre lo que es, si está dentro o no del uso indebido del DNS, aquí estamos para poder comprender la diferencia entre las registraciones maliciosas y las comprometidas.

Entonces lo que vamos a hacer para el resto de esta conversación es ceñirnos a este tema puntual, vamos a tener en cuenta las preguntas o comentarios fuera del alcance para futuros debates, pero yo quiero enfatizar esta cuestión de ceñirnos al tema de la presentación. Pueden hacer preguntas o pueden continuar con el debate en el chat, pero

entiendan la importancia de que nos mantengamos en este tema y lo importante que es para todos.

Bueno, esta es una especie de mapa o estructura de la conversación del día de hoy, tenemos un informe sobre uso indebido del DNS, en el registro o registrador tenemos que hablar de por qué había que hacer una distinción, hay que entrar a un uso o a un proceso de disputas, si no estamos de acuerdo con esto tenemos que hacer entonces la distinción y tenemos que hablar sobre cómo se hace esa distinción, cuáles son los atributos de esta registración para poder hacer la selección correcta.

Después tenemos dos vías aquí a seguir, tenemos un proceso para lo que son los nombres de dominios registrados de manera maliciosa, es decir, aquellos que están destinados o tienen el objetivo de causar daño y en el otro caso, tenemos un proceso para los sitios webs comprometidos.

Creo que, en realidad, lo que tenemos que tener en cuenta aquí como comunidad es focalizarnos en los procesos de los sitios webs comprometidos, pero no más. Entonces tenemos un panel maravilloso el día de hoy, vamos a comenzar con una presentación y a presentar a Maciej quien es profesor de la Universidad de Grenoble y él nos va a dar información, nos va a ayudar a comprender el tema, durará unos 15 minutos su presentación y luego vamos a pasar a una sesión de debate con el panel.

Tenemos gente muy importante, les agradezco a todos los panelistas por formar parte de esta sesión, tenemos a Lori Schulman que viene de la comunidad del IPC, Chris Lewis-Evans del grupo de seguridad pública de GAC, Alan Woods de los registros y registradores, Reg Levy y a Rod Rasmussen del SSAC.

Seguramente ya los han visto antes y nos vamos a dividir en dos sesiones, una va a ser una presentación introductoria, luego vamos a hablar sobre lo que son registraciones maliciosas y luego los sitios webs comprometidos. Después vamos a tener tiempo para las preguntas, pero para todo el debate el pod de preguntas y respuestas va a estar abierto, pero siempre teniendo en cuenta que nos vamos a centrar en el punto de la presentación y si hay alguna pregunta que no tiene que ver con ese tema puntal, las vamos a tener en cuenta para algún otro debate en el futuro.

Creo que eso es todo lo que quisiera compartir con ustedes, esta es una introducción, tenemos expectativas, un alcance y metas claras. Así que, me parece que ahora sí ya es momento de comenzar a presentar, le doy la palabra a Maciej, él nos va a contar lo que está sucediendo en relación a los nombres de dominios registrados maliciosamente y los sitios webs comprometidos. Adelante, Maciej.

MACIEJ KORCZYNSKI: Muchas gracias, Graeme, por la presentación. Hoy vamos a debatir brevemente el problema de los nombres de dominios registrados maliciosamente versus aquellos que están comprometidos. Yo estoy

trabajando en un proceso de investigación y también nos vamos a centrar en la parte técnica de un estudio del uso indebido del DNS hecho por la Comisión Europea, así que, pasemos a la siguiente diapositiva.

Bueno, aquí en la parte superior vemos una URL en la cual pueden ver la descripción de un sitio web malicioso, la pregunta que queremos responder aquí es, ¿este nombre de dominio está registrado maliciosamente? Para responder esta pregunta tenemos que investigar este caso un poco más en profundidad.

Cuando nosotros verificamos el nombre de dominio registrado vemos que en la información de WHOIS fue registrado dos días, antes de que la URL fuera puesta en la lista negra, entonces esto nos brinda cierta evidencia de que el nombre de dominio fue registrado maliciosamente para poder realizar uso indebido o un uso ilegal, por ejemplo, phishing de credenciales.

Entonces, ¿qué es lo que debería hacer un intermediario para mitigar el uso indebido desde el punto de vista técnico? En este caso, tenemos a los registradores o eventualmente el registrador y también el proveedor de servicios de hosting debería intervenir. Esto es importante porque si nosotros suspendemos el nombre de dominio, pero no el hosting malicioso entonces el atacante puede registrar otro nombre de dominio y hacerlo apuntar a ese hosting.

Si solamente suspendemos el hosting, pero no bloqueamos el nombre de dominio, el nombre de dominio puede ser reutilizado por el atacante en otros ataques o en otras campañas de phishing, entonces para incrementar las barreras ante el uso indebido y el costo económico que esto implicaría para otros, se debería hacer una mitigación a nivel del DNS y también a nivel del hosting de estas diferentes partes.

Investiguemos un poco otro caso, aquí tenemos otro nombre de dominio u otra URL maliciosa, esto fue identificado por el grupo de anti-phishing y aquí podemos ver las credenciales en esta página web. La pregunta es la misma, ¿el nombre de dominio está registrado maliciosamente? Hay un sitio web con el contenido y cuando analizamos la información de WHOIS el nombre de dominio fue registrado en el año 2014, probablemente entonces el nombre de dominio en sí sea legítimo.

También cuando miramos el URL malicioso podemos ver que incluye una indicación de que el sitio web ha sido saqueado utilizando una instalación de Word Press. El nombre de dominio es legítimo, pero el sitio web está comprometido y se utilizó para contenido abusivo con violación de marca y con phishing.

¿Cuáles son las implicancias de la perspectiva técnica? En general, no debe haber un TLD registrado que bloquee el dominio porque eso puede causar daño colateral al registrador, a la empresa y también legitimar a los visitantes legítimos del sitio web. La mitigación debe

ocurrir a nivel del hosting, del propietario o administrador del sitio web y de ahí dos cosas para hacer.

Primero, limpiar el contenido malicioso y también poner un patch en la instalación de Word Press. Debe ser entonces un proveedor de alojamiento, si es que el alojamiento está gestionado a través de una plataforma. El proveedor del alojamiento controla todo el software, incluido el software vulnerable o el administrador del web, si tiene un alojamiento no gestionado es el administrador quien va a controlar el software vulnerable, en este caso.

¿Cómo se hace un uso indebido de dominios legítimos? Nosotros en nuestro análisis hemos encontrado que los dominios en líneas generales se utilizan a nivel del website, puede ser un software que explotó un contenido en un sistema avanzado, a veces ocurre al nivel del DNS, un ejemplo aquí sería el shadowing de dominios donde los atacantes primero tratan de encontrar credenciales para robarlas y llegar a su panel de registración.

Una vez que se pueden loguear en el panel de registración pueden agregar, por ejemplo, subdominios que se pueden utilizar en un ataque de phishing. ¿Cuáles son entonces los enfoques existentes para distinguir entre nombres de dominios legítimos y comprometidos de aquellos que son dominios registrados maliciosamente?

Tenemos dos enfoques, el primero, se basa en la heurística, esto se utiliza mucho en informes de la industria, uno es la edad del nombre

de dominio; como se ilustró antes, el tiempo entre la registración y la colocación en la lista negra. También hay patrones de registración, por ejemplo, para ataques de phishing, los nombres o escritos de nombres diferentes pueden ser un blanco de ataque.

Un segundo grupo son los métodos de aprendizaje por máquina, aquí hay una universidad, COMAR, que está financiada por otro organismo y que tiene un enfoque completamente automatizado. Nosotros recolectamos datos vinculados con el alojamiento al sitio web, a la estructura del URL, cuestiones específicas en los nombres de dominios, y extrajimos a partir de allí 38 características que son completamente automatizadas en base a un modelo y hemos demostrado que la precisión es del 97%.

¿Cuál es entonces la relación entre el tipo de abuso y los nombres de dominios comprometidos en contraposición con los maliciosos? Aquí vemos la distribución, los comprometidos en azul y los registrados maliciosamente en rojo. Para el spam, en general, hay que controlar otro aspecto, sin embargo, para el phishing y para el malware este no es el caso, los ataques se pueden lanzar utilizando un nombre registrado maliciosamente o un sitio web comprometido y también servicios gratuitos.

Aquí el 25% de los nombres de dominios y el 41% de los nombres de distribución de malware están registrados por usuarios legítimos, pero seguramente están comprometidos a nivel del sitio web. ¿Cuál es la variación en los distintos tipos de TLD? En la segunda parte del año

2021 hemos observado que para los nuevos gTLD el 98% de los dominios prácticamente fueron etiquetados como registrados maliciosamente.

Si miramos los ccTLD de la Unión Europea a la izquierda vamos a ver que el 42% de los dominios fueron designados como sitios web comprometidos, ¿cuáles son las razones posibles por las cuales esto ocurre? Sospechamos que en la Unión Europea tenemos menos registración especulativa de ccTLD más sitios web con contenido significativo con software diferente que potencialmente puede ser vulnerable y que puede ser explotado a escala.

Aquí entonces vemos la variación en los distintos TLD… Perdón, creo que perdí la conexión, no puedo ver la presentación.

GRAEME BUNTON: Te escuchamos bien.

MACIEJ KORCZYNSKI: No puedo ver la presentación.

GRAEME BUNTON: Es la diapositiva número 13 la que todavía está online.

MACIEJ KORCZYNSKI: Aquí vemos el número total de nombres de dominios que fueron usados inadecuadamente, varios de ellos fueron registrados

maliciosamente, varios comprometidos y en la última columna lo que vemos es el porcentaje de registraciones maliciosas con nombres de dominios que abusan de TLD específicos.

Aquí para ciertos TLD vemos el porcentaje de nombres de dominios registrados maliciosamente, que es de casi el 100%, cabe mencionar el .ML y el .TK donde Freenom da dominios gratuitos a los usuarios y esta es una puerta muy adecuada para los que quieran atacar con phishing.

Por otro lado, vemos también algunos TLD, por ejemplo, como .BR que tiene un 34% de dominios maliciosos registrados y esto puede deberse a varios factores, quiero prestar atención a que esos resultados deben ser tomados con cautela por la limitación en los clasificadores, pero también por las limitaciones de las listas negras en sí que posiblemente no representen la totalidad del ciberespacio.

Algunos proveedores de listas negras pueden concentrarse en los nombres de dominios registrados maliciosamente al utilizar palabras claves identificatorias, etc. Quiero mencionar aquí también que lo que vemos en una lista negra puede ser diferente de un TLD registrado que se ve en una mesa de ayuda cuando se está analizando la queja o el reclamo de la victima de ese ataque, eso se debe a que esas listas negras puedan no ser representativas.

Mi último comentario es que, cada tanto vemos algunas variaciones importantes para el mismo TLD, por ejemplo, .INFO o .COM de un mes a otro, ¿cuál podría ser entonces la razón? Una posibilidad es que uno

de los revendedores da grandes descuentos a los nombres de dominios que son explotados por los atacantes, en este caso, veríamos un aumento en los nombres de dominios registrados maliciosamente y el número total de dominios.

Cada tanto vemos algunas vulnerabilidades que se descubren y que afectan a cientos de miles de nombres de dominios y esto es una meta fácil para los atacantes que pueden explotar a escala, en este caso. En un período de tiempo más corto veríamos la reducción en el porcentaje de nombres registrados maliciosamente versus el nombre total de dominios.

Gracias por su atención, espero que les haya resultado útil el inicio de esta conversación.

GRAEME BUNTON: Gracias, Maciej, usted mencionó varias cuestiones que van a surgir después. En el chat se ha preguntado si esto se puede hacer con algoritmos para detención a través del aprendizaje por máquina.

No sé si vamos a entrar mucho en detalle, pero sería útil que pueda dedicarles dos o tres minutos a los distintos atributos de los nombres de dominios en sí o a los sitios web y, ¿de qué manera las herramientas podrían hacer esto automáticamente o cuáles son las herramientas que los humanos pueden utilizar? Si es que no tienen esa tecnología.

MACIEJ KORCZYNSKI: En cuanto a la primera pregunta, hicimos un análisis de la importancia de las características, el clasificador de COMAR está hecho con un algoritmo de aprendizaje por máquina. Las características que resultan muy útiles son basadas en contenido, por ejemplo, si detectamos en el sitio web que hay muchas tecnologías diferentes que se utilizan cuando se crea el sitio web, esta es una indicación de que el nombre de dominio o que ese sitio web está comprometido.

Por ejemplo, cuando vemos palabras claves como PayPal, pero no solamente marcas, sino otras específicas como verificación. También hicimos un análisis de estas palabras claves y esto es una indicación de que el sitio web está registrado maliciosamente.

Hay cosas que pueden ser capturadas por el clasificador como la cantidad de tecnologías, lo cual es mucho más difícil para un humano. Por otro lado, si queremos hacerlo manualmente hay otras cuestiones como las que vemos en el ejemplo, el tiempo ante la registración y la colación en la lista negra, si es muy corto, en ese caso, será una indicación muy sólida de que el nombre de dominio está registrado maliciosamente.

Si no vemos contenido significativo, el phishing de un sitio web en el nombre de dominio registrado, este es otro indicador de que el nombre de dominio está registrado maliciosamente. Estos dos ejemplos son aplicables a humanos y también al aprendizaje por máquina los puede detectar, es decir, en ambos casos se pueden detectar.

GRAEME BUNTON: Gracias, Maciej. Hay muchos comentarios en el chat, no los puedo seguir porque son demasiados, así que, si tienen alguna pregunta utilicen el recuadro de preguntas y respuestas para que podamos verlas. Hay varias preguntas en cuanto a cómo funciona esta detención.

Algo que pueden mirar es el DNS producido recientemente, algunos de mis amigos pueden ir a encontrar el link en el chat. Yo solo hice una presentación de soluciones de arquitectura el día lunes como parte del día técnico, que creo que da un poco de contexto.

Sé que hay mucho interés en estas tecnologías o en los enfoques humanos para hacer estas determinaciones en las registraciones y ver si son maliciosos o no, pero creo que debemos avanzar al por qué y luego al cómo o al qué.

Esta va a ser mi pregunta para el panel, la pregunta es: ¿Tenemos que hacer esto? ¿Tiene sentido dividir nuestros procesos de mitigación? ¿Tenemos que ver si son comprometidos o no? ¿Es el mismo enfoque para lo genérico o tenemos que tener procesos por separados?

¿Quién quiere comenzar con esta premisa? ¿Tratamos el uso indebido como lo mismo? Empecemos allí y veamos si hay alguien de nuestro panel que quiera responder sobre esto rápidamente.

REG LEVY: Sí, creo que es absolutamente necesario hacer esta distinción, tenemos muchos clientes que utilizan creadores de sitios web que requieren actualizaciones regulares y si no realizan esas actualizaciones muchas veces quedan vulnerables al compromiso.

Entonces conectarse con el registrador, hablar sobre el hecho de que tienen que hacer algo en el nombre de dominio que quizás compraron hace 10 años y no pensaron en los últimos cinco años desde que pusieron el email, que vean su información y tratar de contactarlos, esto es un proceso, tenemos que estar seguros de que la empresa no se vea impactada porque hubo un compromiso en el nombre de dominio.

GRAEME BUNTON: Alan, Chris y luego Lori. Creo que no tenemos que entrar muy en el por qué. Adelante, Alan.

ALAN WOODS: Creo que es importante hacer esta distinción y sé que la razón se tardó muchos años. Desde nuestro punto de vista, como operador de registro, tomamos acciones con dominios donde hay mucho daño colateral y no queremos que haya otra víctima que puede ser el registratario, por eso tiene que quedar muy claro que si vamos a tomar una medida tiene que haber una idea de la precisión.

GRAEME BUNTON: Gracias, Alan. Chris.

CHRIS LEWIS-EVANS: Bueno, quería decir que estoy de acuerdo y que debe ser tratado diferentemente, como dijo Alan, tenemos dos fuentes distintas de daño, lo malicioso versus lo comprometido y también hay diferentes vehículos con lo que está comprometido. También tenemos dos tipos de víctimas, la victima primaria y otras partes que pueden estar siendo afectadas de manera colateral, así que, hay que tratarla y brindar la ayuda que sea suficiente.

GRAEME BUNTON: Muchas gracias. Lori.

LORI SCHULMAN: Yo iba a decir que en la IPC se dice que es importante hacer una diferenciación entre nombres de dominios comprometidos y maliciosos. Rápidamente podemos responder a un tema puntual, pero creo que no deberíamos perder de vista quién es la victima real porque el usuario puede ser el usuario final que está sujeto a un ataque de malware, pero también en el caso de las pequeñas empresas, pueden comprometer su reputación o pueden también ver su negocio comprometido.

No debemos asumir únicamente que el registratario que está administrando le empresa, o cualquier otro negocio, va a preferir tener

el sitio inactivo por algún tiempo porque esto de alguna manera va a afectar a los clientes o su reputación.

GRAEME BUNTON: Muchas gracias, Lori. Lo que tenemos ahora es un equipo dentro de este panel y nadie está en desacuerdo con esta pregunta, que es, ¿hay que hacer o no esta distinción? Así que, ahora vamos a ahondar un poco más en lo que cada una de estas cuestiones significa.

Veo que hay algunas preguntas en el pod de preguntas y respuestas que quizás podemos responder antes de seguir avanzando con el debate. Voy a tomar algunas de estas preguntas y se las voy asignar a los diferentes panelistas. Había una pregunta de Greg Shatan, creo que es para Maciej y preguntaba: "¿Cómo el uso indebido a nivel de servidor de correo electrónico entra dentro del enfoque propuesto?" Maciej, ¿tiene alguna respuesta a esta pregunta?

MACIEJ KORCZYNSKI: ¿Al servidor de correo?

GRAEME BUNTON: Creo que Greg Shatan se refiere al phishing o al malware vía correo electrónico, le pediré que aclare un poco la pregunta. Quizás Greg después pueda acotar algo más en el chat y podemos volver a esta pregunta para responderla.

A ver qué más podemos tratar de resolver antes de avanzar, bueno, hay muchísimas preguntas, por favor les pido que me tengan un poco de paciencia, quiero tomar alguna que sea relevante a esta parte del debate.

La otra pregunta viene de Samaneh para Maciej, pregunta: "¿Las características utilizadas en COMAR también incluyen algunas de estas heurísticas que señaló en el primer método?"

MACIEJ KORCZYNSKI: Bueno, gracias por la pregunta. Nosotros incluimos las características que se utilizan en heurística en esos métodos, además de las registraciones a granel, esa es la única característica que no incluimos y yo diría que hay dos razones.

La razón principal es simplemente que el COMAR debería distinguir malicioso de lo que está comprometido solamente sobre la base de los datos recabados en un caso específico sin obtener información de, por ejemplo, otros nombres de dominios registrados maliciosamente, pero más allá de esto, toda la heurística está automáticamente y plenamente implementada en el sistema COMAR.

GRAEME BUNTON: Muchas gracias, Maciej, hay otra pregunta de Michael Palage para usted, quiere saber su opinión sobre el alto porcentaje de comprometidos en los ccTLD europeos y si eso podría ser atribuido a

un creciente número de ccTLD que hacen verificación de identidad y si esto puede afectar a los datos del registratario.

MACIEJ KORCZYNSKI: Si entendí la pregunta correctamente, la pregunta es, ¿por qué vemos menos registraciones maliciosas y más sitios comprometidos dentro de los sitios web de ccTLD? ¿Correcto?

La respuesta la traté de mencionar durante la presentación, pero nosotros simplemente podemos especular, no podemos hacer ninguna medida porque en lo ccTLD europeos, como se mencionó anteriormente. Tenemos menos nombres de dominios, no tantos nombres de dominios que sean especulativos, hay sitios web detrás de estos nombres de dominios.

Entonces los sitios web y los usuarios también se ocupan de ellos e implementan diferentes softwares porque vemos muchos softwares que se implementan en estos sitios web y algunos simplemente podrían explorar.

Creo que la segunda pregunta tenía que ver con que, ¿por qué se ven menos nombres de dominios maliciosamente registrados? Bueno, esto también es puramente especulativo, hay varias iniciativas a nivel de los ccTLD para evitar las registraciones maliciosas. Como mencioné, en los ccTLD de la Unión Europea hay un sistema similar a Premadoma que detecta a un nombre de dominio que ha sido registrado maliciosamente al momento de la registración u otro ccTLD,

activamente trabajan para poder evitar estas registraciones maliciosas.

Esto es más en lo que respecta a mi experiencia y al proyecto en el que trabajo, pero no quiere decir que en otro ccTLD no se implementen estas cuestiones.

GRAEME BUNTON: Gracias, Maciej. Tenemos muchísimas preguntas en el chat, hay mucho intercambio en el chat. Les pido a los panelistas que, si quieren responder alguna pregunta; ya sea en el pod de preguntas y respuestas o quieren tomar la palabra, que lo hagan con libertad.

A partir de ahora vamos a pasar del lado izquierdo de ese programa que mostramos, ¿cómo sería el proceso para una registración maliciosa? Y las consideraciones en torno a esto, simplemente para garantizar que estamos todos en la misma página. Hablamos de cómo se podría tomar esta decisión, esto es un atributo que quizás tenga el nombre de dominio o una persona que lo esté efectuando y ahora vamos a ver qué tendríamos que hacer.

Entonces a nivel de registro y registrador no hay muchas opciones, pero quizás deberíamos explorar un poco estas opciones y para eso le voy a dar la palabra a Rod. Rod, ¿tiene alguna idea con respecto a las actividades que los registros y registradores deberían hacer en relación al uso indebido del DNS y a las registraciones maliciosas? ¿Tiene alguna idea para compartir?

ROD RASMUSSEN: Sí. Una vez que uno determina o toma la decisión de qué metodología utilizar porque, en este caso, nos vamos a focalizar en las registraciones maliciosas, ¿qué es lo que podemos hacer? Como registro o registrador tenemos muy pocas opciones que tiene el mismo efecto que es, bloquear al dominio del DNS global.

Hay varias formas de realizar esto, uno puede eliminarlo directamente, eliminar esa registración; si tiene una registración maliciosa que se hicieron en los últimos días, hay que estar al tanto de si hay alguna compensación financiera o si quieren que se les devuelva el dinero, pero bueno, hay ciertas cuestiones y quizás se pueden utilizar los mismos registradores para volver al registro. Y esto también de alguna manera podría enfatizar toda esa estructura que tienen, suponiendo que al mismo tiempo alguien también va a mitigar el contenido malicioso, y hay muchos sitios webs comprometidos también, entonces se pueden suspender.

Por otro lado, el nombre de dominio, no se elimina, pero se entra en un estado de suspensión, se remueve del DNS e independientemente del plazo de esa registración está en un estado de suspensión, eso es algo que no hay que gestionar. Y después hay otras medidas de mitigación activas que se pueden tomar también.

Durante muchos años el grupo de trabajo de anti-phishing ha brindado una página de inicio donde ustedes pueden ver los sitios con phishing,

allí pueden ver si hay un ataque de phishing y si esto está siendo redireccionado a otros lados o si está apuntando a diferentes partes también en el caso del malware, se puede recibir información y esto da la posibilidad de informar a las víctimas de que están comprometidos de diferentes maneras, puede ser a través de los proveedores, puede ser una compañía de seguridad o para una agencia de cumplimiento de la ley que tome acción concreta y efectiva también para las víctimas de malware para que sepan que son infectadas.

También se puede transferir el nombre de dominio a otra entidad, ya sea desde la perspectiva del registratario, por ejemplo, el FBI toma dominios, también lo hace Microsoft y se puede utilizar el registrador de último recurso que se estableció o se establece para tomar el control de los nombres de dominios que se utilizan para malware y brindar esa información de manera automática a las víctimas.

Es decir, hay diferentes opciones a tener en cuenta, pero esto también implica cierto trabajo en garantizar de que haya un proceso implementado para poder llevarlo a cabo y, además, una vez que se ha decidido o se determina que hay un nombre de dominio malicioso, quizás sería buena idea ver si hay otros nombres de dominios que están alineados o que están siendo utilizados por quizás la misma cuenta de registratario teniendo en cuenta que esa cuenta es muy importante.

Creo que Reg y otros panelistas van a hablar luego de la importancia de entender si una cuenta fue establecida por un actor o si está

comprometida porque quizás alguien puede ser víctima de phishing o tiene problemas con las credenciales. Por otro lado, hay buscar si se ha creado un patrón en las diferentes partes para ver si hay uso indebido a lo largo de un ámbito mayor de nombres de dominios en las cuentas del registratario.

Eso podría también derivar a una campaña a gran escala, pero estos actores son sumamente inteligentes y suelen esconderse de aquellos registradores que son muy diligentes en tratar de identificar todas estas cuestiones problemáticas.

GRAEME BUNTON: Muchas gracias, Rod. Para resumir brevemente, los registradores tienen entonces tres opciones por así decirlo, los registros también pueden participar, pero uno puede borrar, puede suspender o bien puede señalar o redireccionar y habría diferentes razones para llevar adelante estos tres pasos y también hay que verificar la cuenta, hay que ver si cumple con algún otro patrón.

Son todos aportes muy interesantes para la gente que trata de mitigar el uso indebido. Quisiera saber si Alan o Reg tienen algún otro punto de vista sobre cómo implementar estas cuestiones y por qué se deben implementar o no, ¿qué es lo que piensan? Lori, adelante por favor.

LORI SCHULMAN: Gracias. Tengo una pregunta sobre lo que dice Rod, sobre los patrones del abuso y buscar una gran cantidad de ejemplos. En las condiciones

que tenemos hoy sobre la legislación y las políticas actuales, ¿la investigación solamente está restringidas a registradores? O puede quizás haber un espectro más amplio de registradores donde los registros sean quienes hagan la investigación y no los registradores.

GRAEME BUNTON: ¿Rod?

ROD RASMUSSEN: Sí a ambos. Un registrador tiene la capacidad única de poder ver que hay cuestiones que están siendo expurgadas de la información pública, lo cual es un activo muy valioso al hacer este tipo de heurística que se estaba mencionando antes, que lo mencionó Maciej. También tienen la posibilidad de ver que hay tarjetas de crédito que se están utilizando y que se están haciendo ingresos en cuentas.

Y un registro tiene una muy buena idea de un patrón que está ocurriendo, especialmente si soporta un algoritmo de generación de dominio, que es un malware, donde un conjunto de dominios se registran para generar un comando y control de malware, lo vemos en distintos registradores y hay allí un patrón, también pueden analizar cuestiones como el alojamiento de DNS y la forma en la que un dominio queda configurado, por eso se pueden mirar en los servidores principales de DNS o un IP alojado virtualmente y, en general, se puede detectar este tipo de cosas.

Se le puede preguntar a los registradores sobre lo que hacen y si es que esto es legítimo.

GRAEME BUNTON: Gracias, Rod. Chris, voy a ir a Reg y a Alan antes de volver a usted, pero antes de avanzar con este tema; y hablamos de lo comprometido, me da curiosidad saber si desde la perspectiva de la aplicación de la ley en las registraciones maliciosas donde uno, en general, está conforme con esa interrupción o para una registración maliciosa hacen una investigación para saber más del proceso, pero Reg y otra persona brevemente, luego vamos a pasar al lado más comprometido y luego las preguntas y respuestas.

REG LEVY: Gracias, soy Reg Levy de Tucows, que también es un registrador. Nuestra forma de enfocar todo esto va a ser bastante distinto de un registrador que tiene una relación directa con el registratario, trabajamos con nuestros revendedores y buscamos patrones de revendedores. Cuando hay mucho abuso que proviene de un revendedor en particular, nos conectamos con ellos y les decimos: "Hey, somos expertos en ocuparnos de el uso indebido del DNS, ¿cómo los podemos ayudar?"

Generalmente esto se resuelve de esta forma. También tenemos un revendedor interno y cuando vemos muchos dominios maliciosos registrados que vienen de ellos podemos tomar una medida directamente contra el registratario, siempre que sea una parte

identificable. Como se ha mencionado en el chat, los que hacen fraude no usan su nombre o el mismo nombre para varios dominios, hay que buscar este tipo de patrón y muchas veces eso no es muy útil.

Luego miramos dónde se registra el dominio para ver si es malicioso o es comprometido, sí, lo hacemos. Lamentablemente mucha inteligencia artificial que se menciona también en el chat, le faltan cosas o tiene un espectro muy alto para las bajas, tenemos que hacer mucha verificación respecto de lo que la inteligencia artificial nos presenta.

Una de nuestras historias favoritas tienen un dominio de generación de dominio, un tonto registró las mismas letras que estaba utilizado el DGA y fue un acrónimo muy largo para una agrupación de mujeres que fueron al futbol en América Central y entonces el registro tuvo que permitirle registrarlo. De nuevo, este es un ejemplo de este tipo de algoritmos basados en computadora que van a utilizar demasiado de la red.

GRAEME BUNTON: Alan y luego Chris para poder avanzar.

ALAN WOODS: Esta es la forma en la que el registro debe avanzar, todo lo que Reg dijo, cuando ella habla con un revendedor está hablando con los registratarios. Creo que es muy importante que desde el punto de vista del registro miremos esos indicadores y vamos a ver si alguien lo

puede hacer para mí hasta cierta medida, pero tiene que ver con el escalamiento basado en la evidencia y tiene que haber conversaciones con los registratarios.

Podemos centrar una conversación de detección de la cual yo quiero salir porque quiero hablar de lo que está comprometido y cómo identificar lo comprometido, es un aspecto importante. Hay que pedir también desde el punto de vista del registratario, como dijo Lori. Yo creo que hay muchas grandes empresas que estarían completamente en desacuerdo y hay que dejar muy en claro cuál es la proporcionalidad, si el daño es causado al registratario o al usuario final más.

Creo que hay que hacer declaraciones más amplias y definitivamente tiene que haber una proporcionalidad.

GRAEME BUNTON: Gracias, Alan, esto va a ser una buena forma de entrar al próximo componente de nuestra discusión y vamos a entrar a eso en breve, después de escuchar a Chris.

CHRIS LEWIS-EVANS: Sí, a fin de cuentas hablamos de malware y de phishing aquí, o sea que tiene que haber una investigación y seguramente no es una sorpresa para nadie que, en general, no registran un solo dominio. El dominio estará bajo investigación y los registros, registradores o proveedores de hosting deberán cambiar a un trabajo proactiva o reactivo, esto va

a evitar que haya más víctimas y más daños. Siempre la aplicación de la ley busca maneras de evitar que todo esto ocurra.

GRAEME BUNTON: Muy bien, tenemos 35 minutos y quiero que respondamos las preguntas, hay mucha actividad en el chat, gracias a todos por esa participación.

Hicimos el trabajo fácil hasta ahora, que es ver cómo hacer esta distinción, hablamos de cómo, hablamos también de qué hacer en la circunstancia de una registración maliciosa y ahora tenemos el otro lado, que es donde se complica y es donde hay el ejemplo del uso indebido del DNS, por ejemplo, malware, phishing, en un sitio web comprometido.

El sitio web es benigno en sí, puede ser una pequeña empresa, puede ser una más grande, puede ser un blog de alguien también. ¿Cuál es el proceso que se debe aplicar en esta circunstancia? ¿Cuál es el daño que se puede estar generando? Tenemos, de nuevo, una pregunta para Reg y Alan, que es: "Si se determina que un sitio web está comprometido, hay phishing, malware y uso indebido del DNS, hay una circunstancia en la que uno lo tiene que dar de baja y que no esté online? Es decir, ¿hay que suspender el dominio en un sitio web comprometido?"

¿Alan?

ALAN WOODS: Pareciera que la proporcionalidad tiene que ser mágica, tenemos que ser muy claros como registradores que tenemos instrumentos muy directos en un sitio web, en un dominio, en el email asociado con ese dominio. Para que el registro diga: "En esta instancia no tengo respuesta del registrador ni del registratario y el daño, que objetivamente es grande, está ocurriendo todavía". Sí, siempre hay un punto donde podemos tomarlo en cuenta, pero hay que tomar en cuenta la proporcionalidad del daño.

Me emociono, voy a dar un poquito más de espacio para los intérpretes. Estamos hablando sobre cosas que son difíciles para la vida humana, como el material de abuso sexual, cosas que son excepcionales.

Y tiene que quedar muy claro que el registro no debe ser el punto donde se da de baja todo lo que es posible, pero cuando sea necesario tenemos esa posibilidad.

REG LEVY: Nosotros tendemos a utilizar la suspensión como opción de último recurso para dominios comprometidos, nos contactamos con el revendedor y el registratario directo, y les decimos: "Hay algo que pasó, ustedes los pueden solucionar". Y en base a la respuesta o no respuesta podemos empezar a resetear varios registros, uno por uno, para luego dar de baja al email primero, si es ahí donde ocurre el compromiso.

Reiniciar el servidor de nombres y a veces hay que ver si ese email es algo a lo que yo tengo que responder y que lo tengo que solucionar, lo cual es otra parte en la que muchas veces tenemos que permitir que el dominio se resuelva para que puedan loguearse en el sitio web y resolver el problema.

Suspender el dominio va a evitar el uso malicioso, pero no va a permitir ningún otro uso, ni tampoco la mitigación del uso indebido.

GRAEME BUNTON: Gracias Reg y Alan, pro ese input.

Lori, Rod, Chris, ¿hay alguna información que ustedes creen que debe ser incluida en ese test que se hace con los registradores? Esa verificación del daño que se debe elevar, si es que la gente está pensando qué hacer con un sitio web comprometido, para cuando uno se involucra en el uso indebido del DNS.

LORI SCHULMAN: Voy a responder primero por lo que ocurre en el chat. Creo que tenemos que ampliar la conversación, pero esta vuelve a algo que Reg explicó, con lo cual yo estoy de acuerdo.

Cuando miramos los nombres de dominios comprometidos, esto es lo que yo quería decir en el chat porque hay algo que quedó como súper interpretado, miramos entonces un camino de decisión muy diferente

en cuanto a cómo y cuándo lo vamos a hacer porque hay una participación de un sitio web que está operando, que está ofreciendo un servicio o algún otro tipo de beneficio, que si suspendemos un dominio se va y esto puede incluir los ingresos de alguien.

Pero lo que yo estoy tratando de decir aquí es que; y esto va a lo que dice Rod y Alan, ¿de qué estamos hablando cuando hablamos de phishing o malware? ¿El sitio quedó comprometido porque hay pornografía? Me voy a referir específicamente a la pornografía infantil. Hay casos claros en los que hemos decidido como comunidad que no infringen porque en mi propia práctica muchas veces un sitio está comprometido y después empezamos a ver CSAM en el sitio.

Hay empresas más grandes y empresas más pequeñas, las empresas más grandes tienen distintos caminos de decisión y cómo responder a algo, quizás en el interés de estas empresas nosotros no tenemos que tener CSM asociado con estos dominios, esto tiene que parar ahora, tenemos que reiniciarlo, resetearlo. Este es mi punto.

No podemos tener una solución que funcione para todo en los nombres de dominios comprometidos… Perdón que esté hablando muy rápido, voy a desacelerar un poquito, pido disculpas. Lo que voy a decir más lentamente es que, hay árboles de decisiones con matices que se deben tomar con los dominios comprometidos, no se pueden hacer suposiciones sobre lo que el propietario de una empresa quiere o no quiere decir.

Con respecto a lo que dijo Alan, no debemos descontar los casos extremos y, sin duda, no debemos descartar, y agradezco lo que hace Tucows porque es muy comunicativo con sus revendedores y les hace saber qué es lo que está ocurriendo.

Creo que una parte importante del problema del equilibrio es que, tenemos consideraciones de tiempo dependiendo de cuánto daño se está haciendo y cómo, luego tenemos la consideración de los registratarios que pueden decidir si es en el mejor interés tener o suspender estos dominios para poder resetearlo y que el marketing, la publicidad, en ese dominio no se diluya. Esta es una palabra de las marcas, pero tiene que haber una entidad respetable y tenemos que ver cuáles son los compromisos que ocurren en esa práctica.

Espero haber hablado más lento.

GRAEME BUNTON: Gracias, Lori, por el comentario. Tengo a Chris, a Alan y después tengo una pregunta que quisiera plantear al panel. Adelante, Chris.

CHRIS LEWIS-EVANS: Bueno, para mí en cuanto a los nombres maliciosos y dentro del grupo de partes interesadas de registros y registradores, tenemos estándares que se requieren para la mitigación de usos indebidos y esto es distinto para los nombres de dominios comprometidos, así que, la idea es permitir a los registros y registradores actuar sobre ciertos estándares de evidencia para los dominios comprometidos.

Como informador o persona que hace informes de uso indebido se contacta al registrador, a la empresa, y se toma acción. Después el debate se centra en cómo esto se hace, pero si tomamos el malware hay muchos informes que se hacen. Una única infección de ransomware podría, por ejemplo, implicar el fin de un negocio para algunos casos, así que, poder articular estos estándares de evidencia.

Recientemente tuvimos muchas operaciones, muchas actividades y la idea de poder articular todo esto, diciendo: "Hay que contactar al registrador, a la persona". Bueno, no sucedió nada, no hay respuesta, entonces volvemos al registrador o al registro y le pedimos una suspensión por estas razones, eso hace que se ponga en marcha un proceso de decisión.

Y también comprendemos que probablemente haya que debatir. Empresas multinacionales cuya suspensión podría causar un problema mucho mayor, el phishing también puede llegar a determinadas personas y tener un impacto masivo, así que, le pedimos que vaya al registrador, le damos 48 horas para responder y después hacemos la solicitud. Creo que es un debate muy largo, pero se reduce al daño causado por el nombre de dominio comprometido y el daño colateral también, se requiere recabar más evidencia por parte de quienes realizan sus informes y también el compromiso de las diferentes partes que están involucradas en la cadena para que tomen acciones al respecto.

GRAEME BUNTON: Muchas gracias, Chris, hay muchos comentarios. En este tema en particular pienso que tiene toda la razón, que hay mucho trabajo por hacer dentro de este espacio todavía y también estamos rápidamente pasando responsabilidades o experiencias de los registros y registradores en lugares como, por ejemplo, las empresas de hosting, pero, Alan, le cedo la palabra primero, antes de ir a la pregunta.

ALAN WOODS: Voy a ser muy breve en mi comentario. Tenemos el documento SAC-115 que habla de la interoperabilidad y de garantizar que los operadores específicos estén o participen rápidamente para tener una respuesta oportuna. Así que, creo que ahí es momento de actuar, cuanto más rápido actuemos menos daño ocurrirá y muchas veces se tratan de evitar daños, la idea es buscar espacios o [introducir] el backend y trabajar.

Lo importante a señalar es que, algunos registradores, por supuesto, son registradores de plataformas muy grandes que tienen procedimientos para mitigar el uso indebido muy sofisticado. Entonces no vamos a eliminar o a cancelar, por ejemplo, a FACEBOKK.COM, no vamos a bajar o a cancelar FACEBOOK.COM porque eso sería ridículo, Facebook tiene sus procedimientos, pero creo que tendríamos que tener un equilibrio en ese sentido.

GRAEME BUNTON: Muchas gracias, Alan. La pregunta que surge en diferentes oportunidades se la voy a hacer a Alan y a Reg otra vez porque esto requiere quizás cierta elaboración por parte de la comunidad, es: "¿Qué tipo de relación tienen los registros y registradores de los Estados Unidos con las empresas de hosting? Porque mi idea es que hay muchos que piensan que es una relación muy cercana, yo no quiero hablar por ustedes, pero me parece que hay muchas otras circunstancias en las que las cosas no son así.

Hablamos de la complejidad de toda esta cuestión, Chris habla de un camino o de una vía de escalación donde hablamos del registrador, las empresas de hosting y el registro, son esas intervenciones y relaciones claras, ¿hay un proceso claro para establecerlo? ¿Cuál son los pasos a seguir?" Reg.

REG LEVY: Bueno, mi respuesta va a ser teniendo en cuenta que Tucows es un registrador mayorista y puede diferir de lo que sucede en otros registradores, nosotros tenemos cientos de sitios webs, así que, básicamente nosotros decimos que no tenemos hosting, nuestros revendedores, por lo general, son también empresas de hosting, así que con frecuencia nosotros nos contactamos con un revendedor y decimos: "Hay un sitio web comprometido". Y ellos se ocupan sin ni siquiera tener que contactar al registratario.

En el caso de que ese revendedor sea una empresa de hosting sí tenemos ese tipo de relaciones, una relación muy cercana, pero no

siempre es así, hay muchas empresas de hosting también donde el hosting es un servicio que requiere un nombre de dominio, peor está completamente separada del servicio de brindar nombres de dominios y sus registraciones.

Entonces en caso de que un revendedor no sea una empresa de hosting nosotros usamos las mismas herramientas de otros usuarios de internet para ver quién es la empresa de hosting y bueno, confiamos en la información que podemos obtener, y nos contactamos, contactamos a esa empresa de hosting.

GRAEME BUNTON: Bien, gracias, Reg. Alan, tiene la palabra ahora.

ALAN WOODS: Y, nuevamente, disculpas a los intérpretes por mi ritmo al hablar. Desde el punto de vista del registro es mucho más difícil, nosotros no tenemos esa conexión con los proveedores de hosting, probablemente esperamos que esto se haga antes de que lleguen a nosotros le podemos pedir a nuestros amigos los registradores ver si pueden contactarse con el proveedor de hosting, pero lo que voy a acotar es que, nosotros sí nos relacionamos en gran medida.

Hay diferentes aspectos de esta conversación, está el tema de los contactos de los que habla la ICANN, también el tema de la jurisdicción porque en este debate también hay proveedores de hosting que no están fuera del debate porque están fuera de la jurisdicción, entonces

tenemos que tener este tipo de conversaciones. Es importante para nosotros tomar estos aprendizajes, llevarlos a la comunidad y creo que estamos haciendo bastante con respecto a esto que está sucediendo en la definición de la jurisdicción e internet.

Trabajar con proveedores de hosting no siempre es posible, es un paso importante para todos nosotros como registros y registradores.

GRAEME BUNTON: Muchas gracias, Alan. Hay muchos registradores que quizás son empresas de hosting, pero no todos y determinar un hosting o también tener una relación con esos hosting en todo el mundo no es algo sumamente común y esto es un impedimento que tenemos que empezar a analizar para ver cómo mejorar estos procesos de informe y así podemos tener más herramientas a nuestra disposición, ser más proactivos a la acción.

¿Y cómo definimos este camino o esta vía de escalación para los registros y registradores cuando no hay una respuesta por parte del registratario o del host para hacer el informe de uso indebido? Nos quedan unos 18 minutos, veo que Lori ha levantado la mano, después vamos a tratar de responder algunas de las preguntas de la sección de preguntas y respuestas. Adelante, Lori.

LORI SCHULMAN: Yo quería hacer algunos comentarios siguiendo lo que se decía en el chat. En cuanto a la [confección] del informe y nuestra posibilidad

de… Es importante traer a este debate cuándo es necesario o razonable… Y cuánto se debería esperar en este [espacio], ya sea para la implementación de tecnologías de mitigación o de seres humanos, por ejemplo, la inteligencia artificial tiene redes muy puntuales y aún así se sigue necesitando la presencia humana para verificar la actividad de la inteligencia artificial, no todo se puede dar por sentado.

Así que, entendemos que un internet más segura; o al menos mi Unidad Constitutiva lo entiende, requeriría más inversión y quizás esto implicaría precios mayores, y a veces no queremos hablar de eso. Esta es una inquietud particularmente para la Sociedad Civil donde es importante el precio de los nombres de dominios, que sigan manteniéndose a un bajo costo. Y, al mismo tiempo, sabemos que hay ciertos registros y registradores que están invirtiendo cada vez más.

Me parece que esa es una pregunta importante que la comunidad podría plantearse.

GRAEME BUNTON: Bueno, gracias, Lori. Y probablemente esa sea un camino o un punto para nuestra próxima pregunta, es decir, ¿cuál es el rol de esta comunidad? ¿Hay un rol que tenga la ICANN para tratar de abordar estos desafíos que acabamos de descubrir el día de hoy? ¿Podría haber mejores prácticas implementadas para las registraciones maliciosas? ¿Cuál es el enfoque que tiene la ICANN sobre los sitios webs comprometidos? ¿Cuál es el lugar que tomaría la comunidad?

Yo no voy a hablar desde el punto de vista del DNS, pero me pregunto si alguien en el panel quisiera ver hacia dónde va esta comunidad, le voy a dar la palabra a Rod… Reg levantó la mano, adelante por favor.

REG LEVY: Sí, yo creo que el equipo de cumplimiento de la ICANN tiene un ámbito dentro de los contratos para poder exigir ciertas cuestiones cuando no se toman las medidas necesarias para mitigar el uso indebido del DNS, si está dentro del contexto de la ICANN esto no va a implicar el contenido legal o el CSAM para el uso indebido del DNS, pero la ICANN debería también aprovechar esto, es decir, utilizar esas cláusulas contractuales y hacerlas exigir.

GRAEME BUNTON: Gracias, Reg. Le doy la palabra a Rod y luego a Chris.

ROD RASMUSSEN: Hay una pregunta parecida en el recuadro de preguntas y respuestas. El SSAC ya habló sobre esto en el SAC-115, la comunidad y la organización, incluidas las partes contratadas y todos los que participan, a tener una conversación, pero es un tema más amplio.

Nosotros estamos focalizados entre comillas en el abuso del DNS y algunos de los desafíos que tenemos son, ¿cuáles son los proveedores de servicios adecuados que deben estar involucrados en mitigar esta cuestión maliciosa y cuáles son los daños? ¿Cómo se mitigan esos daños? ¿Cuáles son los estándares de la evidencia, de las pruebas?

¿Cuáles son las expectativas sobre el reconocimiento y la mitigación del uso indebido informado?

Hay muchos temas y estamos viendo un movimiento hacia iniciativas más grandes, como el instituto de uso indebido del DNS, ese es un trabajo que está haciendo jurisdicción e internet y se está tratando de crear prácticas estándares, pero todavía tenemos un camino largo por recorrer en tratar de crear un único ecosistema en el que la gente pueda tener expectativas en torno a los proceso, la proporcionalidad y lo otro que se necesita para crear una mejor respuesta al uso indebido.

Como comunidad de la ICANN podemos estar de acuerdo, pero luego conectarnos con el resto de la comunidad más amplia en cuanto a cómo enfrentar estos temas porque si todos tratamos de resolver nuestra parte del rompecabezas vamos a tener muchos sistemas distintos, ICANN quizás puede tener un rol en fomentar las conversaciones porque tiene muchos otros esfuerzos que no necesariamente tienen todo esto en el email o en los dominios. Los aliento a que lean el documento SAC-115 y que participen en la conversación, sean proactivos, piensen globalmente cómo enfrentar estos problemas y crear los marcos que necesitamos para fijar las expectativas y luego seguirlas.

GRAEME BUNTON: Gracias, Rod. Creo que alguien mencionó el SAC-115 en el chat. Chris y luego Alan.

CHRIS LEWIS-EVANS: Estoy de acuerdo con todo lo que se ha dicho, hemos avanzado enormemente en cómo enfrentar el uso indebido del DNS, no creo que tengamos un proceso adecuado para enfrentar los dominios comprometidos, tener unas expectativas mínimas y lograr que esto se documente nos tiene que permitir medir las respuestas. Esto sería muy útil, que esos estándares sean presentados a registros y registradores, y también poder educarlos.

Hay muchos tipos diferentes de registros y registradores, entender las mejores prácticas y cómo hacerlo es central, hay mucho que ICANN puede hacer en ese sentido y luego poder también generar el camino, hacer campañas a los proveedores de servicios y ser una parte central de todo lo que está ocurriendo.

GRAEME BUNTON: Alan brevemente y luego vamos a responder algunas preguntas.

ALAN WOODS: Brevemente. Ocurre que, como parte de este proceso e incluso antes de tratar de sugerir este plenario, el grupo de partes interesadas de registros y el sub grupo de DNS trató un proceso y Graeme está involucrado en esto como líder no oficial porque yo no estoy, hasta que incorporemos gente del SSAC también, queremos incorporar a Rod y a otros para tener luego una conversación muy robusta sobre lo malicioso versus lo comprometido y hacer exactamente lo que Chris ha dicho, que es establecer el camino.

Esta es una conversación abierta, esto es reconocer que hay un problema, sabemos que hay un uso indebido del DNS y estamos trabajando en eso, pero también el trabajar en los matices, en las diferencias para enfrentar esto más efectivamente. Con suerte vamos a tener algo sólido para empezar pronto.

GRAEME BUNTON: Gracias, estamos trabajando en ese documento y creo que lo podemos tener listo alrededor de la reunión de La Haya, en junio, creo que estaríamos más cerca de junio que de ahora. Lo vamos a circular en la comunidad.

Hay una pregunta en el chat sobre un tema, "¿qué puede hacer la comunidad en cuanto al RAA? ¿Qué se puede aplicar para capturar algunas de estas buenas prácticas o temas de los que hablamos hoy?" Potencialmente esto está sobre la mesa, yo recibí una carta del instituto del uso indebido del DNS, hay un pequeño equipo que se ocupa de esto y hace esta pregunta, lo estuve haciendo yo mismo.

El rol de la comunidad aquí es morder una pequeña parte de esta manzana en este ecosistema, especialmente donde el uso indebido está comprometido, hay nombres de dominios comprometidos. Creo que tenemos que comenzar con lo que tenemos más cerca del lado de lo malicioso, ¿cuáles son las consecuencias? Si es que son más pequeñas, si hay menos víctimas.

Creo que podemos comenzar a pensar cuál es el rol de la comunidad en las registraciones maliciosas y creo que esto también está establecido en los estatutos de la ICANN. Esa sería mi sugerencia y espero haber respondido la pregunta de Fab en el chat. Tenemos siete minutos más, quiero darles la oportunidad de hacer comentarios o si hay preguntas también, si alguien quiere preguntar directamente. Reg, levantó la mano, adelante.

REG LEVY: Quería decir algo que se dijo en el chat. El grupo de partes interesadas de registros está trabajando en una herramienta donde podemos poner un nombre de dominio y va a incluir información sobre quién es la empresa de alojamiento y cómo contactarla, lo presentamos en la reunión del grupo de partes interesadas de registros esta semana y esperamos que esté disponible pronto.

GRAEME BUNTON: Gracias, Reg, es importante y es algo similar en lo que está trabajando el instituto de uso indebido del DNS porque queda claro que todos estos procesos identifican todos los componentes en el ecosistema, quiénes son, cómo contactarlos, cuáles son las normas, las formas para contactarlas. Podemos hacer un mejor trabajo de resolver los problemas para contactarse. Yo estoy trabajando en algo como esto, este no es el lugar para hablar de esto, pero voy a compartir noticias sobre este tema muy pronto.

A ver si podemos responder un par de preguntas, pido disculpas por no ver el excedente de preguntas que estamos teniendo, vamos a ver si podemos responder algunas preguntas sobre el tema que estuvimos hablando hoy. Lori.

LORI SCHULMAN: El chat va muy rápido y no lo puedo seguir. Quiero decir que este panel es muy oportuno y era muy necesario, quiero agradecerles a los organizadores por haberme invitado, haber invitado al IPC y a mí en particular porque pone de relieve los temas complicados, yo no creo que nadie esté diciendo que esto es fácil, esto no es un tema fácil.

Nadie está diciendo que tenemos que tomar decisiones rápidas, pero sí creo; al menos donde yo estoy sentada, que específicamente con los nombres de dominios comprometidos hay quienes trabajan en la ley, en la ciberseguridad y ellos conocen estos temas desde hace tiempo, hay instancias de uso indebido que pueden tener un remedio que sea mejor o peor. Si este uso indebido va a ser analizado con su propio conjunto de hechos.

A mí me queda claro que nosotros como comunidad debemos establecer las normas y ahí es donde los proyectos como el I&J o el de Graeme nos ayudan a establecer este problema, pero tenemos que ver de qué manera las normas que se establecen por fuera de la comunidad funcionan dentro de la ICANN también. Voy a poner una sugerencia en el chat que ya ha sido discutida en mi Unidad Constitutiva y es que, cuando tenemos el problema de la

ciberocupación; cuando apareció ese tema hace 20 años, no había un sistema judicial para ayudar con estos casos, hemos encontrado puntos en común y desarrollamos el UDRP que funcionó muy bien durante 20 años.

Quizás ya sea el momento de pensar en un proceso parecido al UDRP para los dominios comprometidos, se los dejo aquí sobre la mesa, pero me parece que es una pregunta para el futuro y para la solución de normas que debemos considerar.

GRAEME BUNTON: Gracias, Lori, por ese aporte. Brevemente, antes de pasar a Alan, ya hablamos de lo que ocurre dentro de la comunidad, pero también tenemos un instituto dedicado a este futuro. Para mí es muy obvio que los temas del uso indebido salen por fuera del alcance de la ICANN muy rápidamente y tenemos que contactarnos con el proveedor del alojamiento, tenemos muchas organizaciones como Global Cyber Alliance, I&J, topDNS, ECO que trabajan de formas parecidas, que trabajan en resolver algunos problemas.

Lo que nosotros tenemos que hacer es poder ver cómo trabajar en conjunto, colectivamente, respaldamos el modelo de múltiples partes interesadas en la ICANN y vemos mucha importancia en este trabajo. Debemos entender también que hay un lugar para las organizaciones adyacentes que pueden ir más allá de sus límites y trabajar con la comunidad de un modo que quizás no sea adecuado para la ICANN o para las reglas dentro del sistema de la ICANN.

Poder explicar a quienes están por afuera, a reguladores en el mundo, a la ICANN y a la comunidad que hay un lugar para que ambos trabajen, hay cuestiones contractuales y PDP, etc., pero también que la industria pueda desarrollar buenas prácticas, conectarse con hosting, con proveedores de email. Todo esto puede colaborar y funcionar en conjunto, tenemos que simplemente mejorar en hacer esto porque se pueden resolver una gran cantidad de estos problemas.

Tenemos un minuto más, Alan, quizás tiene la última palabra.

ALAN WOODS: Quiero hacer eco de lo que usted dice, Graeme. Es importante decir que no estoy en desacuerdo con Lori, de hecho, estoy muy de acuerdo con mucho de lo que dice y tenemos que garantizar que el UDRP se ocupe de los nombres de dominios y aquí estamos hablando de lo que dice Graeme, que es mucho más amplio y simplemente no solamente son registros y registradores, sino que es algo mucho más amplio que la ICANN, pero sí las partes constitutivas de la ICANN trabajan con otros y hacen su parte para completar esto.

Me parece que, literalmente, esta es la forma en la que estamos impulsando esto, tenemos que entender que esta es un área interoperable, tenemos que tener el apoyo y la comprensión de todos, y estamos mejorando. Creo que debemos continuar mejorando aún más.

GRAEME BUNTON: Gracias, Alan. Hemos llegado al final de nuestra hora, quiero agradecerles a nuestros panelistas, les agradezco por tomarse su tiempo. Maciej tuvo una muy buena presentación, gracias a la audiencia que ha sido excelente por respetar nuestro foco y hubo muchos más aportes de los que podríamos haber recibido, pido disculpas por eso, vamos a tratar de capturar todos los aportes y ver si hay alguna forma de incorporarlo en alguna otra sesión o en algún otro trabajo.

Con eso, creo que podemos terminar nuestra sesión, gracias a todos por su participación, es muy valiosa.

**[FIN DE LA TRANSCRIPCIÓN]**