ICANN82 | Foro de la comunidad – Reunión conjunta: GAC y SSAC
Domingo, 9 de marzo de 2025 – 16:30 a 17:30 PST

NICOLÁS CABALLERO: Señoras y señores, bienvenidos. Por favor, tomen asiento. Empiecen la grabación.

GULTEN TEPE: Hola y bienvenidos a la reunión del GAC de la ICANN 82 el domingo 9 de marzo a las 16:30 hora local. Esta sesión se está grabando y se rige por las normas de conducta esperada de ICANN y también por las políticas antiacoso.

Durante esta sesión, las preguntas y comentarios que se pongan en el chat se leerán en voz alta si se ponen en el formato apropiado. Recuerden decir su nombre y el idioma en el que van a hablar si van a hablar un día que no sea el inglés. Por favor, hablen con claridad y a un paso razonable para permitir una interpretación precisa y asegúrense de silenciar sus dispositivos cuando vayan a hablar. Pueden tener acceso a todas las características disponibles para esta sesión en la barra de herramientas de Zoom. Con esto le doy la palabra a Nicolás Caballero, el presidente.

NICOLÁS CABALLERO: Bienvenidos a la última pero importante sesión, por lo menos en mi humilde opinión, con el SSAC, Comité Asesor de Seguridad y Estabilidad. Bienvenido, Ram y a su fantástico equipo. Estábamos hablando acerca de uno de las cuestiones de las cuales vamos a hablar. Lo hablamos ayer y anteayer. Cuando yo hablé acerca de computación cuántica y el impacto en el DNS y la estabilidad y la implementación del DNSSEC, y la criptografía en general asimétrica y demás, todos me miraron como si estuviese loco. Puede ser el caso.

Vamos a hablar acerca de ese tema en detalle con este equipo de expertos. También vamos a hablar acerca de computación cuántica y su impacto en el encriptado, como mencioné en el día de ayer. También hablaremos acerca del estudio INFERMAL. Para el beneficio de los nuevos miembros del GAC, yo ya expliqué eso pero vamos a hablar de eso en detalle. Después hablaremos acerca de los pasos a seguir. Bienvenido, Ram y a su equipo fantástico. Le doy la palabra.

RAM MOHAN: Muchas gracias, Nico. De parte del SSAC les extiendo mucho aprecio al GAC por esta invitación. Esta es la tercera vez que hemos estado con ustedes. Cada vez que lo hemos hecho, la interacción ha sido más enriquecedora. Hay más participación entre nosotros. Valoramos esta oportunidad para fortalecer nuestro diálogo colaborador con respecto a asuntos que tienen que ver con seguridad y estabilidad de Internet.

Para ustedes que son nuevos en el GAC y en la comunidad de ICANN, brevemente les cuento que el SSAC sirve como el organismo de expertos asesor de ICANN y se dedica a analizar amenazas potenciales en lo que tiene que ver con los sistemas de nombres y direcciones de Internet.

Se compone de expertos técnicos y proporcionamos recomendaciones en base a evidencias a la comunidad de ICANN y la junta. Cuando nosotros no damos recomendaciones basadas en evidencias, en esos casos tratamos de mostrar que son opiniones de expertos que estamos presentando a la comunidad y a la junta.

Nuestro enfoque abarca un gran espectro de vulnerabilidades del DNS, riesgos en ciberseguridad y también el impacto en la infraestructura y la seguridad y la estabilidad y la resiliencia en lo que tiene que ver con gobernanza de Internet. Fundamentalmente nuestras responsabilidades están dentro del área de infraestructura crítica y ahí es donde participamos nosotros.

Entendemos que el rol vital del GAC de representar las perspectivas gubernamentales con respecto a la gobernanza de Internet junto con otros temas, entendemos que esto permite que el SSAC pueda unir los dominios técnicos y de política. Nuestro deseo en continuar esta participación es asegurarnos de que nuestras recomendaciones sean robustas y que se alineen con el interés público. Ese es el enfoque clave.

Queremos compartir nuestras perspectivas, escuchar sus comentarios y continuar asegurando la estabilidad, resiliencia y

seguridad de Internet. Eso es lo que nos impulsa a hacer este trabajo y por eso agradecemos la participación con el GAC.

Tenemos dos temas que queremos hablar con ustedes. Russ Housley está aquí, a mi derecha. Russ tiene una carrera larga y distinguida. Entre otras cosas, él pasó bastante tiempo fijándose en la computación cuántica y el impacto en el encriptado. Tenemos aquí a Russ para compartir sus opiniones en cuanto al tema.

Nuestra intención no es darles una disciplina. Más bien es pedir que ustedes compartan con nosotros sus pensamientos y que participen o interactúen con nosotros. No queremos que nuestras presentaciones sean muy técnicas, aunque el material en realidad básico sea técnico. Si hablamos de pronto de una manera muy nerd o técnica, por favor, simplemente díganlo y pregúntennos qué queremos decir con lo que decimos. Ahora le doy la palabra a Russ.

RUSS HOUSLEY: La computación cuántica ha existido ya por un tiempo y el Instituto Nacional de Tecnología y Normas hizo una gran competición. La solución que salió de eso se llama ML-DSA, que es un algoritmo de firma digital basado en lattice, una estructura modular.

Esto no encaja bien con el DNSSEC. Es muy grande. Tiene claves públicas y valores de firma. Si uno usa el DNS sobre UDP, no funciona. Las buenas noticias de eso, sin embargo, es que tenemos tiempo porque la inquietud más grande que tenemos con la

computadora cuántica es lo que nosotros llamamos el ataque de harvest ahora, decrypt después. El punto es que si hay muchos secretos y se guarda, tenemos una computadora cuántica encriptada. Pueden atacar las claves, conseguirlas y revelar los secretos.

En el DNS no existen secretos. Eso no es un problema. Nuestra inquietud en este tema es que tenemos una firma digital que no se puede falsificar a tiempo cuando llega el punto de necesitar una mitigación en cuanto a la existencia de una computadora cuántica. La segunda diapositiva habla acerca de tal vez alguna de las cosas que pudiéramos hacer. Siguiente diapositiva, por favor.

Lo que pudiéramos hacer para poder utilizar estas firmas cuánticas. Esta es la investigación que está en progreso. Está el grupo de trabajo de Internet, que se fija en el porqué del DNSSEC. Es una respuesta a muchas cosas como, por ejemplo, el blockchain, firma transparente y otras cadenas. No nos sorprende que ellos sean la base. Puse aquí varios enlaces en la diapositiva. Uno habla acerca de firmas basadas en hash de estado para el DNSSEC. Esas firmas de pronto se podrían utilizar, que también son bastante grandes, junto con otras técnicas.

La próxima semana, en el IETF 122, vamos a hablar más acerca de ese tema pero no espero aún la respuesta de aquí a un año. Tenemos tiempo. Si tienen alguna pregunta en cuanto a esto, no sé si hacemos las preguntas en este momento o las dejamos para el

final. No. Si hay alguna pregunta en este momento, con mucho gusto se la contestaremos.

NICOLÁS CABALLERO: Gracias. Por favor, para el beneficio del GAC completo, explique qué son las firmas digitales.

RUSS HOUSLEY: Sí. Una firma digital es en lo que se basa el DNSSEC. La idea es que cuando uno consigue una respuesta a su consulta, la firma digital se adjunta a eso. Quiere decir que no se ha cambiado desde cuando originalmente se publicó. Es lo que provee la integridad y la autenticidad de los datos en sí.

NICOLÁS CABALLERO: Muchas gracias. Ahora tenemos aquí a los Países Bajos.

MARCO HOGEWONING: Gracias. Soy Marco, de los Países Bajos. Gracias por una vista general. Breve pero profunda en cuanto al tema. Todavía nos falta mucho por hacer. Sé que a veces pensamos que tenemos bastante tiempo pero no es así. Es más corto de lo que pensamos. Sin entrar en detalle técnico, ¿hay algún consejo concreto que nos pueda dar a nosotros, los gobiernos, en este momento? ¿Qué podemos hacer para prepararnos para lo que tal vez va a ser un momento inevitable donde vamos a tener que cambiar el algoritmo del DNSSEC?

RUSS HOUSLEY: Para el DNSSEC todavía es muy pronto. Para otros protocolos de seguridad sí tenemos unas soluciones. Hemos trabajado en otros grupos de trabajo de IETF como LAMPS, que trabaja en el PKI y SMIME. Tenemos TLS. Tenemos IPSEC. En esas cuatro áreas tenemos soluciones donde la infraestructura se tiene que utilizar en este momento para que cuando lo necesitemos esté presente porque va a tomar unos años.

Si reflexionamos cuando ocurrió la transición de SHA-1 a SHA-256, yo era el director de área de seguridad en ese entonces. Yo pensaba que cinco años iba a ser suficiente tiempo. Tomó el doble del tiempo. Comiencen con la infraestructura para que la transición pueda ocurrir porque no pueden ocurrir muchas otras cosas después si no existe una infraestructura a la que conectarlo. Ese es mi consejo.

NICOLÁS CABALLERO: Steve, adelante.

STEVE CROCKER: Russ, creo que sería bueno hacer un seguimiento a esa pregunta. Tiene mucho sentido una pregunta sobre qué pueden hacer los gobiernos. Habló acerca de la transición de SHA-1 a SHA-256. ¿Me puede hablar más en cuanto a cómo se va a haber esa transición cuando ocurra la decisión de cómo va a ser ese nuevo algoritmo, o si el cambiar a ese algoritmo va a ser diferente cuánticamente al

compararlo con lo que ya hemos tenido o lo que tendremos? De pronto es un cambio en el algoritmo donde ya tenemos la práctica y la experiencia.

RUSS HOUSLEY: No lo sabemos con seguridad. Esa es la respuesta. Lo que sí sabemos es que esta vez es más complicado porque no estamos simplemente cambiando una pieza de una caja sino que estamos cambiando la caja completamente. En esa situación, hay que verlo de esta manera, si estamos hablando de una KPI, estamos hablando de construir uno desde la raíz, desde abajo hacia arriba. No simplemente cambiar las piezas sino cambiarlo en su totalidad. No sé si eso ayudó. Si no, disculpe.

NICOLÁS CABALLERO: Gracias, Steve, por la pregunta. Gracias, Russ. ¿Hay alguna otra pregunta? ¿Algún comentario? Yo sí tengo una pregunta para usted, Russ. Digamos que el gobierno X tiene una buena implementación de DNSSEC y de MANRS y RPKI. Cualquier combinación de Blowfish y RSA y DES o SHA-256 o cualquier combinación de esas cosas. De repente existe un avance en la computación cuántica. Me corrige si me equivoco pero en ese caso ese gobierno con la estructura de DNSSEC va a ser algo automáticamente obsoleto. ¿Tengo razón en decir eso?

RUSS HOUSLEY: Sí, pero no queda claro cuándo va a ocurrir eso. Hay mucha bibliografía que estamos viendo acerca de avances en la cantidad de qubits y en computación cuántica pero, por el momento, estamos lejos de algo que sea relevante desde el punto de vista criptográfico. Estas cosas no son lineales. Se producen avances de asaltos en distintas medidas. Cuando estas cosas ocurran van a ocurrir. No podemos responder eso ahora. No es algo lineal. Tanto RPKI como DNSSEC son muy singulares en cuanto a que solo necesitan integridad. No hay ninguna cuestión allí. No hay secretos que recoger. Tenemos más tiempo allí porque no hay una capa de decriptación de los registros que nos preocupe.

NICOLÁS CABALLERO: Entonces deberíamos estar bien. Hay una buena combinación de DNSSEC, RPKI y MANRS.

RUSS HOUSLEY: Sí. Simplemente tenemos más tiempo para resolver esos problemas porque solo incluyen datos públicos y tenemos integridad.

NICOLÁS CABALLERO: Gracias. Tenemos a Australia y a Países Bajos.

INGRAM NIBLOCK: Sé que cumple con diferentes propósitos pero quisiera saber si puedo hablar acerca del rol de DNS sobre HTTPS y DNS sobre TLS.

Podemos pasar a los nuevos algoritmos. El tema de seguridad, transporte. ¿Vamos a obtener los beneficios que estamos obteniendo actualmente con DNSSEC por medio de esta capa de transporte encriptada?

RUSS HOUSLEY: Sí y no. Sí. Van a proteger el tráfico entre el punto de encriptación y el de desencriptación. Es un sistema que va hub por hub cuando uno lo aplica al DNS de esa forma. Esto nos va a ofrecer protección. Como dije, el trabajo sobre TLS está en curso. Todavía no tenemos la PKI para integrarla pero con el navegador tendremos resultados después de la semana que tendrá lugar en Tokio con el grupo de acción de ingeniería de Internet.

NICOLÁS CABALLERO: Gracias, Australia. Gracias, Russ. Por el bien de los nuevos miembros del GAC, quiero aclarar que PKI es infraestructura de clave pública. MANRS es normas de seguridad de enrutamiento mutuamente acordadas. Podemos después darles todos los enlaces para que puedan acceder. Tengo a Países Bajos y después el caballero que está allí. Perdón, no sé su nombre. Primero Países Bajos.

MARCO HOGEWONING: Gracias, Presidente. Si damos un paso lateral, estoy tratando de evitar que esto sea un debate demasiado técnico pero en la diapositiva anterior usted mencionó los desafíos que tenemos con

el transporte de UDP. Recuerdo que esta no es la primera vez en la industria del DNS que nos encontramos con límites en cuanto a UDP como transporte. Creo que también esto se presenta en la implementación actual con respecto a la implementación de DNSSEC. Considerando que estamos mirando un horizonte de largo plazo, ¿sería posible considerar distintas opciones de transporte para el DNS más allá de UDP?

RUSS HOUSLEY: Otras opciones de transporte son opciones que conocemos y que están especificadas. Simplemente no están implementadas. Como parte de esta transición, quizá sí se implementen.

MARCO HOGEWONING: Vuelvo a hacer la pregunta. Nosotros, los gobiernos, ¿cómo podemos ayudar?

RUSS HOUSLEY: Buena pregunta.

NICOLÁS CABALLERO: Russ, ¿podría darnos dos o tres ejemplos de cómo remplazar UDP?

RUSS HOUSLEY: DNS sobre TCP, DNS sobre QUIC, DNS sobre TLS. Estos son ejemplos que no tienen las mismas limitaciones por mensaje.

NICOLÁS CABALLERO: Muchas gracias. Países Bajos, Adelante.

PETER THOMASSEN: Peter Thomassen, miembro de SSAC. Me parece que algunas de las cosas que se dijeron, pueden decirse de una forma menos técnica. Es lo que estoy tratando de hacer. Russ dijo antes que las firmas están adjuntas a las respuestas del DNS y testifican que la información del DNS no se ha modificado desde que fue publicada. Por supuesto, si todos pudieran adjuntar una firma, eso no sería muy útil. Para adjuntar una firma es necesario tener control de una clave privada y para eso necesitamos una firma.

La computación cuántica está tratando de falsificar estas firmas. Tenemos también la encriptación, que trata de proteger datos secretos para que no sean elegibles, a menos que uno tenga la clave de encriptación. Esta también es una aplicación de claves.

Es importante reconocer que la computación cuántica es una amenaza para ambas aplicaciones, tanto las firmas computacionales con firmas, y también la encriptación y desencriptación. Pero son diferentes casos de uso. El DNS no se ocupa de la encriptación y la desencriptación sino que le preocupa verificar en el momento en que uno trata de conectarse y hacer una consulta al DNS, verificar que esa firma sea válida.

Si uno quiere quebrar eso con computación cuántica, tendría que hacerlo en muy poco tiempo, casi en tiempo real, mientras que si

uno logra registrar, encriptar información de una transferencia de HTTPS, como teníamos en el pasado, podemos tardar cinco años en desencriptar eso.

Si tenemos una computadora cuántica lenta, podemos trabajar con los datos encriptados pero no sería una amenaza para la información del DNS, porque si toma cinco años acceder a la firma, a esa altura ya nadie le va a interesar esa información porque, de otra forma se puede hacer en cuestión de segundos.

El mensaje con respecto a lo que podrían hacer los gobiernos, que creo que es la pregunta que hizo Países Bajos, con respecto al DNS, no se asusten. Es un problema de investigación por el momento. Es una buena idea hacer un seguimiento del tema, creo, si les interesa.

El problema más inmediato es proteger los datos secretos almacenados o en tránsito que es el mismo problema de extracción de la clave pero es más urgente y también se están haciendo más avances allí que en el campo del DNS. Quería aportar eso.

RUSS HOUSLEY: Muchísimas gracias por dirigir la sesión la semana que viene.

RAM MOHAN: Nico, quisiera ofrecerle a usted y al GAC lo siguiente. Si hay alguien que tiene algún proyecto inicial en esta área, por favor, contáctense con nosotros y podemos darles algo de material que quizá podría resultarles útil a sus miembros cuando ustedes trabajen con sus gobiernos. Creo que aquí hay una diferenciación

útil para entender y transmitirles a otras personas en sus gobiernos cuál es la parte negativa de la computación cuántica y DNSSEC con respecto a la computación cuántica y secretos compartidos.

NICOLÁS CABALLERO: Muchas gracias, Ram. Muchas gracias, Russ. No estoy totalmente seguro con respecto a ese marco de cinco años que usted mencionó, Peter. Gracias por la explicación. Realmente espero que no pero creo que podríamos encontrarnos con sorpresas en el futuro cercano. De todas formas, antes de darle la palabra a Jeff quisiera saber si hay alguna otra pregunta, alguien que esté aquí en la sala o alguna pregunta remota. No veo que nadie pida la palabra. Muchísimas gracias, Russ. Vamos a pasar ahora a Jeff, a quien le voy a dar la palabra.

JEFF BEDSER: Gracias, Nico. Soy Jeff Bedser, de SSAC. Se hizo una pregunta para que habláramos acerca del estudio INFERMAL. El estudio INFERMAL fue creado por la oficina del CTO de la ICANN. El área de investigación tiene investigadores académicos que analizan las registraciones maliciosas en cuanto a dominios utilizados para cometer uso indebido online, principalmente phishing.

Una de las primeras cosas que tengo que advertirles, y lo puse en negrita en el siguiente párrafo, es que este no es un informe que ofrece soluciones sino que está diseñado para responder preguntas planteadas por la comunidad desde hace tiempo acerca

de la influencia de determinados factores con respecto a dónde obtienen los delincuentes cibernéticos los nombres de dominio para cometer ataques.

Tenemos incentivos económicos, verificación proactiva, restricciones estrictas que servirían para mitigar el uso indebido de dominios. Tenemos un informe publicado en noviembre del año pasado. Pasamos a la siguiente diapositiva, por favor.

¿Cuáles son hallazgos clave para aquellos de ustedes que no leyeron el informe? Tenemos la parte de incentivos económicos, una tarifa de registración más baja. Cada dólar que se reduce en las tarifas de registración corresponden con un 49 % de aumento en dominios maliciosos. Servicios gratuitos, disponibilidad de este tipo de servicios como alojamiento web, genera un aumento del 88 % en las actividades de phishing.

Descuentos. Los descuentos en las registraciones de dominios están asociados con un gran aumento en las registraciones maliciosas y con respecto a las medidas proactivas que se pueden tomar, tenemos restricciones más estrictas con respecto a esos dominios que pueden reducir el uso indebido en un 63 %. Acceso a la API, que es la posibilidad de realizar adquisición de muchos dominios al mismo tiempo. Esto puede representar un 401 % de aumento en los dominios maliciosos registrados y, por supuesto, prácticas de verificación. La verificación proactiva de información de registratarios como dirección de correo electrónico, validación

de teléfonos. Eso significativamente reduce las registraciones maliciosas. La siguiente diapositiva, por favor.

Cuáles son las medidas reactivas. Tiempo de mitigación. El impacto de los tiempos de mitigación sobre la reducción del uso indebido del dominio es mínimo. Incluso un breve tiempo puede servir para que los atacantes puedan acceder a credenciales valiosas y ganancias financieras, registradores y preferencias de TLD, concentraciones de uso indebido, registraciones maliciosas que no se distribuyen en forma uniforme y que tienden a estar concentradas en determinados registradores y TLD, y prácticas de registradores. Los registradores ofrecen precios bajos y servicios gratuitos.

Esta es información que está validada, que ya existe entre la comunidad de uso indebido desde hace mucho tiempo. El tema simplemente se llama ganancia económica. Los compradores van a donde pueden comprar al precio más bajo, donde pueden comprar grandes cantidades. Hay muchos lugares en el mundo donde hay grandes entidades que venden grandes cantidades de todo tipo de productos y que venden a un precio más bajo.

Si bien esta es una lectura legítima de los datos, no implica necesariamente una resolución del problema porque si uno sube el piso al precio, igual va a existir un precio más bajo considerando las diferentes economías del mundo, las diferentes monedas y no vamos a eliminar el problema de esta manera.

Además, tenemos las pérdidas por delitos cibernéticos. Yo he visto números que van desde un trillón hasta 10 trillones. Yo creo que estos son valores posibles. La diferencia entre un trillón y 10 trillones es un número muy grande si hablamos de pérdidas. La mayoría de los estudios muestran a nivel global. La pérdida promedio por phishing es 136 % en el global. Sin embargo, en Estados Unidos ese número sube a una pérdida promedio por phishing de 3.520 dólares.

He visto variantes de todos esos números. Seguramente aquellos que trabajan en esta área conocen muy bien esos números y saben que dependen de cada estudio, pero la realidad es que si cada pérdida representa como mínimo 136 dólares, esto hace que los que ganan mucho dinero con el delito cibernético no quieren dedicarse a actividades que no son delictivas.

Tenemos que ver cuáles son las políticas, cuáles son los cambios que podemos implementar para mitigar o reducir el problema de las registraciones maliciosas que se utilizan para cometer delitos cibernéticos, para perjudicar a la gente, para robar dinero. Si cambiamos el precio, ¿esto va a cambiar los incentivos de los delincuentes para ganar cientos de miles de dólares? Si el dominio pasa de costar dos dólares a 10 dólares por año. Lo planteo como pregunta. La siguiente diapositiva, por favor.

El proceso de verificación, una vez más, tal como señalé, el estudio se publicó en noviembre. Está basado en datos de ese momento. Los temas de inteligencia artificial continúan acelerándose a un

ritmo que excede el ritmo al que avanza la computación cuántica pero en este momento, la capacidad de crear identidades generadas digitalmente, uno puede tomar el nombre real de una persona y decirle a un algoritmo de inteligencia artificial: “Necesito una licencia para conducir, para esta persona, para este país, con el mismo formato pero con el nombre de una persona real de la misma edad y que tenga una foto que se parezca a la mía” o “utilice mi foto para poder generar digitalmente una identidad que luego pueda utilizarse en un proceso para registrar un dominio”.

Esto afecta mucho a la capacidad de decir: “Si solo verifican la identidad de cada registrador, van a resolver la problema”. Las probabilidades de diferenciar algo falso de algo real con una foto, ya no es: “Vamos a precisar la inteligencia artificial para hacer esa diferenciación, para distinguirlo”, porque ya los seres humanos no lo pueden hacer. ¿Cuáles son los mejores procesos que nos servirán para que los dominios no se registren de forma fraudulenta, más allá de los procesos de verificación manual?

También existen problemas en cuanto a la detección de delegaciones, mitigaciones. Si es una medida válida. Lo que estoy sugiriendo aquí es que la mayoría de los estudios que se han hecho utilizan los recursos disponibles públicamente en cuanto a los volúmenes del uso indebido del DNS. Son cifras que produjeron shock.

El problema más grande del uso indebido del DNS y del phishing en particular es que se basan en las entidades, que lo vean e intenten

reportarlo. En este momento, los informes generados en este tema se fijan en estas cosas dañinas. Cuántos de ustedes ven un phishing en su celular y piensan: “Ah, esta vez no me cogiste” y borras eso.

Quiénes de ustedes más bien lo han reportado. Si lo han hecho, los elogio pero no creo que haya muchas manos. El problema es que si no se reportan, entonces no están visibles a la industria para que los puedan mitigar. Por eso cambiar la metodología en la registración es una solución pero también hay mejores oportunidades para poder detectar esto, para poder mitigarlo inmediatamente, para que si aparece un dominio por seis o siete segundos, se puede inmediatamente remover. Más bien si dura dos días, alguien lo reporta y toma dos días para validarlo, ya son cuatro días. Más bien queremos detectarlo más rápidamente para removerlo inmediatamente.

Obviamente, en cuanto al otro punto de medición, algo que ya deberíamos estar haciendo, pero mirar en los números de víctimas por dominio, porque uno puede tener 100 víctimas en un segundo por un phishing muy bien hecho. No es necesariamente el número de dominios que están haciendo el phishing sino las víctimas que caen en esa trampa.

Sabemos que si estamos hablando del punto más alto del iceberg, que es un recurso disponible que habla del phishing, vemos el volumen de esto, pero hay muchos que no se reportan y no se ve. Hay mucho más en cuanto a poder reportar el verdadero impacto por víctima para ver el efecto financiero.

Hablo de esto porque nos da este informe. INFERMAL valida bien. Precios más bajos impulsan bien. El precio más bajo para los registratarios impulsa ese phishing. ¿Cómo llegamos al siguiente paso? ¿Qué podemos hacer para mejor medir el impacto y cómo podemos mejor detectar esto para ser más eficaces en parar este problema?

Yo diría que aunque empecemos a cobrar más, por ejemplo, 1.000 dólares por dominio por año, lo que realmente estamos haciendo es más bien eliminando la habilidad de la persona de tener un dominio en Internet debido al costo pero no hacemos nada con los ciberdelincuentes que ganan todavía. Van a tener todavía un margen de ganancia. Hay que buscar una solución. Gracias.

NICOLÁS CABALLERO: Gracias, Jeff. Eso es lo que iba a decir. Por favor, pongan la siguiente diapositiva. El aumento de 400 %. Me encantaría tener esa conversación en este momento. El tema de API, el interfaz de aplicación de programación. Realmente, ¿ese es el problema de que los maleantes tienen acceso a la API y al usar la inteligencia artificial o lo que sea entonces son más capaces de causar daño y aumentar las actividades de phishing? ¿Ese es el caso?

JEFF BEDSER: No tengo duda de que esa registración es un vehículo para gran acceso a uso indebido. El 401 %. Por ejemplo, un actor malo que está registrando estos dominios o estos algoritmos para un botnet,

una campaña de malware, puede estar registrando 10.000 dominios en un momento y eso no hace que el API sea malo porque el porcentaje en base a la API puede ser un usuario comparado con varios usuarios en un API.

Por otro lado, si llegase a haber espacios donde alguien registra 50 dominios, de pronto pregunten: "¿Será que esos dominios que se están registrando se van a usar para algo malo?" Hay mucha información de infraestructura para averiguar si se va a utilizar para eso o no. Que sean 10.000 a la vez, yo diría que no es así. Yo diría que más bien el problema es la falta de restricción.

NICOLÁS CABALLERO: Gracias. ¿Alguien tiene algún comentario o alguna pregunta de los miembros del GAC o de los que están participando por Internet? No veo ninguna mano alzada en el salón. No, disculpe. Sí, hay dos manos. Está India y Australia. Cuando pueda, India, por favor.

SUSHIL PAL: Yo creo que es claro que la verificación es un problema. Si tenemos las credenciales verificadas de los registradores, entonces la probabilidad del uso indebido del DNS no es tanta o se reduce. No es la inteligencia artificial el problema, sino las credenciales que no se verifican y que se comparten a través de las API.

El problema es claro. Todavía tenemos que averiguar con GNSO cómo definir la veracidad de los datos y el ámbito de los datos porque si no desistimos en el ámbito de la veracidad de los datos

del WHOIS, entonces nunca podremos verificarlo. El SSAC quizá pueda instar a la GNSO que acelere el proceso en cuanto a esto. Si no, no podemos dar un paso adelante para poder restringir eso.

JEFF BEDSER: Algo en lo que quizá no fui claro en mi presentación es que las personas que están utilizando el dominio para este propósito, con quienes estamos batallando en contra, están a 10 o 100 pasos adelantados a nosotros. La tendencia reciente es que son personas legítimas con credenciales legítimas, crean una cuenta y a través de los meses crean un portafolio de dominios y los venden con esas credenciales a un delincuente, quien después utiliza esos dominios para propósitos malos. Aunque se implica mejor fricción con una mejor verificación de credenciales, sí ayuda, pero mi punto es que si nosotros nos basamos mucho en eso como en una solución, ese es un problema.

La otra inquietud real es que esta es una sesión pública y les garantizo que las personas con las que estamos batallando ya van a ver esto. Se van a enterar de esta información y ya van a decidir cuáles son los pasos a tomar para seguir con la delincuencia. Cuando hablamos acerca de qué podemos hacer, tiene que ver con lo que vimos en la diapositiva anterior. Se trata de tener una mejor detección. La aceleración en el proceso de mitigación es la idea. No podemos tener un incentivo económico porque los delincuentes siguen todavía robándoles a las personas a pesar de esto pero si pudiéramos averiguar cómo hacerlo donde la persona lo hace,

cogemos a la persona y minimizarlo por lo menos, minimizarlo hasta cierto punto. Esos incentivos ya no existen. No sé si me entienden. El punto es que hay que buscar una mejor detección y mejores tasas de mitigación. Es lo que va a ayudar a estos problemas.

SUSHIL PAL: Cuando hablamos de la verificación, no estoy diciendo que esta sea la solución completa pero es un paso a dar. Sé que estamos hablando y hablando de esto pero no estamos dando un paso adelante en cuanto al lado de la verificación. En los ccTLD donde operamos, por ejemplo, en nuestro país, nosotros tenemos un proceso de verificación de dos pasos y significativamente se ha reducido estos usos indebidos. Es un gran costo que tenemos debido a estos ciberataques. Es importante para nosotros reconocer que el primer paso hay que tomarlo. No queremos menospreciar la importancia de la detección y adquirir capacidades para monitorear esto.

NICOLÁS CABALLERO: Gracias, India. Tengo a Australia, la Comisión Europea, el Reino Unido y los Países Bajos. Vamos a seguir con Australia.

INGRAM NIBLOCK: ¿Cuáles son los pasos en cuanto a la investigación del estudio INFERMAL? Estamos fijándonos en las características de los registradores, ¿pero hay una manera de validar esta hipótesis con

los registradores? Porque tenemos dominios en particular que tienen en su lista de bloqueo y lo que utilizan en su investigación pero en escala de pronto conseguir datos utilizables en cuanto a qué están haciendo estas personas en estas instancias de uso indebido y qué datos tiene supuestamente el registrador. Creo que estos serían pasos a tomar en la investigación en sí.

JEFF BEDSER: Sí. Tendría que referirlo hacia la oficina del CTO en cuanto a sus informes y los próximos pasos a tomar. Lo que le podría decir aquí. Quizá no es una respuesta apropiada lo que le estoy diciendo.

NICOLÁS CABALLERO: Gracias, Australia. Ahora la Comisión Europea.

GEMMA CAROLILLO: Mi colega Martina Barbero ya habló del tema del uso indebido del DNS en el chat. Vamos a tener una presentación del informe en la sesión del uso indebido del DNS y también con la intervención de OCTO. Dejaré que ellos hagan las preguntas. Tengo dos preguntas. Una es una pregunta general. Como este informe de INFERMAL tiene mucho eco y hemos escuchado sus comentarios en ciertos aspectos, ¿tienen ustedes alguna declaración con respecto a los comentarios del informe a los que podamos acceder con respecto al uso indebido del DNS o ciertos aspectos del informe? Esto nos va a ayudar a poder leer el documento.

Mi segunda pregunta es que yo entiendo que el problema en sí no es API pero ese es el caso en cualquier cosa en la tecnología. Como la registración en bulto es el problema, ¿qué debemos entender? ¿Que deben existir restricciones en cuanto al uso del API? Quizá tratar el tema de lo que tiene que ver con estas registraciones en bulto.

JEFF BEDSER: Esto no viene de un documento de SSAC en el momento. Este documento de consenso no viene del SSAC. Podemos conseguir un consenso en cuanto a qué pasos tomar con respecto al informe de INFERMAL. La segunda pregunta, disculpe, se me olvidó.

En cuanto a los datos de registraciones masivas, yo creo que hay una corporación, por ejemplo, que está estableciendo una nueva marca o identidad y tiene que registrar esa misma entidad a través de varios TLD. Pueden ser 2.000 registros en ese momento. Esas herramientas tienen un propósito válido en esa instancia.

Es difícil para mí en una cantidad más alta, puede hacer el caso de lo que tiene que ver con estas registraciones masivas. Hay reglas para conseguir, por ejemplo, una licencia para manejar una motocicleta o para manejar un automóvil. Hay diferentes reglas para manejar un camión. Hay que conseguir diferentes licencias dependiendo de la capacidad de uno para lesionar a otra gente si opera el vehículo mal. Uso ese ejemplo para mostrarles que la herramienta de API es similar al ejemplo que yo puse de un cambión, donde uno necesita pasar por un proceso más vigoroso.

Por eso no se trata de la herramienta en sí sino la licencia que se da a la persona para utilizar esa herramienta.

NICOLÁS CABALLERO: Tiene la palabra el Reino Unido.

NIGEL HICKSON: Esto ha sido sumamente interesante, poner este informe importante en contexto y que SSAC lo analice. Quiero agradecérselo. Me preguntaba si esto podría continuar y quizá convertirse en una recomendación o algo así, considerando la importancia de estas recomendaciones que ustedes publican ocasionalmente. Gracias.

RAM MOHAN: Gracias, Nigel. No llegamos todavía al punto en el que definimos o decidimos si tenemos que hacer una recomendación al respecto. La oficina de OCTO hizo una presentación ante SSAC sobre este tema también pero lo que no hicimos fue mirarlo y decir: ¿Hay algo extra por encima? En parte se debe al hecho de que parte del trabajo que se hace aquí cae más bien dentro de la parte de desarrollo de políticas de la ICANN y no tanto dentro de la parte de asesoramiento técnico.

El informe INFERMAL brindó bastante asesoramiento técnico pero esto es lo que yo pienso aunque no hemos tenido un debate específico dentro de SSAC sobre este tema. Gracias por la sugerencia. Lo vamos a plantear cuando tengamos la próxima

conversación dentro de SSAC para ver qué opinan los miembros de SSAC.

NICOLÁS CABALLERO: Gracias, Ram. Países Bajos pide la palabra.

MARCO HOGEWONING: En términos de mitigación, este es un problema de política. Jeff habló acerca de mejorar la detección y mejorar la API. Me pregunto si fuera de los debates sobre políticas tendríamos que hablar acerca de los estándares técnicos que podrían mejorarse para poder mejorar la detección y resolver parte del problema. ¿Hay espacio para soluciones técnicas?

RAM MOHAN: Voy a hablar brevemente y después quizá Jeff pueda agregar algo. No sé si hay una solución técnica necesariamente pero sí hay un componente de educación. Cuando uno recibe un phishing o un smishing, ¿sabemos qué hacer? No solamente cómo detectarlo sino cómo informarlo, denunciarlo.

Uno de los problemas que tenemos a esta altura dentro de nuestra comunidad es que si no se denuncia, entonces no podremos recopilar los datos suficientes como para poder decir: “Hubo mil cosas informados”. Un 10 % son casos a los que no se respondió de una forma determinada. Veamos ese 10 % o sea cual sea el porcentaje. Veamos quién está detrás de eso.

Veamos cuáles son los patrones para tratar de entender cuáles son las conductas, las características dentro del ecosistema. Algo práctico sería llevar a cabo una campaña de educación sólida que diga: “Denuncie el uso indebido, denuncie el phishing, denuncie esas cosas”.

Una vez que se haya hecho esto podemos ir y hacer un seguimiento de lo que se hizo en adelante. Luego podremos contar con datos que nos darán un foco real del problema, de dónde podría estar el problema o quién podría estar contribuyendo al problema. Por el momento estamos en un modo en el que con frecuencia tratamos de aplicar un abordaje general. Creemos una política que se aplique a todos. Pintemos a un grupo de actores determinados de una forma en particular cuando tenemos actores dentro de ese grupo que hacen un trabajo excelente y otros hacen un trabajo muy malo. Creo que el foco debería estar en aquellos que no llegan al nivel adecuado. Una vez que contemos con los datos podremos decir que esta son las mejores prácticas, estas son las normas que hay que cumplir. Creo que las mejores prácticas se pueden llevar a cabo y se pueden crear sin desarrollo de políticas porque estamos diciendo: “Esto es obviamente algo bueno para tener un mejor ecosistema, un ecosistema más sano”.

JEFF BEDSER: No tengo nada más que agregar.

NICOLÁS CABALLERO: Gracias, Ram. Creo que la República Dominicana pidió la palabra.

AMPARO ARANGO: Es un panel muy importante. Sí. Muy técnico. Muy, muy técnico pero creo que está en el corazón de lo que estamos enfrentando hoy en día en nuestros países. Quiero hablar aquí como gobierno y como un país pequeño, la República Dominicana. Algo al final lo estaba diciendo usted. Qué debemos hacer. Qué tenemos que hacer nosotros como gobierno. Primero saber cuál es la situación en nuestros países, en nuestros propios administradores de dominio, en nuestros operadores. Yo vengo del regulador de telecomunicaciones. Nuestros operadores. Todos nuestros centros de ciberseguridad, nuestros centros de respuesta a los ataques porque hemos tenido en los últimos años…

Costa Rica el año pasado acaba de pasar hace dos años una situación terrible, que le costó millones y millones de pesos. Atacaron todo su sistema de salud. Nosotros hemos tenido cosas allí. Un poco desde la perspectiva de nosotros como gobierno, y a lo mejor ustedes no lo pueden decir así tan claro pero creo que necesitamos estrategias, orientaciones más claras de cómo promover esto del DNSSEC en nuestros países. Qué tantos actores conocen esto del DNSSEC. Qué tantos no lo conocen. Nuestros operadores, nuestros centros de ciberseguridad, nuestros propios administradores de dominios. Yo no sé si es el de mi país lo tiene o no lo tiene.

Creo que por ahí está la clave de cómo ir atacando este problema de ciberseguridad y de inseguridad que teníamos tan grande. Me gustaría escuchar recomendaciones pero creo que esto va a ser entre SSAC y también nosotros como GAC. Porque al final esto lo tenemos que convertir en herramientas concretas para que podamos… Es regulación, es educación, es costoso, es muy costoso tener una estrategia nacional para tener todos nuestros sistemas con DNSSEC. Trato de hacer como esta reflexión. No sé si me la pueden contestar pero me angustia esto. Creo que tenemos herramientas para por lo menos mitigar estos impactos. Gracias.

RAM MOHAN: Gracias. Qué pregunta importante. Uno de los desafíos que tenemos en SSAC es que podemos ofrecer muchos conocimientos técnicos e información técnica pero lo que no comprendemos totalmente bien y lo que no tenemos es cuáles son sus necesidades. Qué nivel de información necesitan.

Tenemos que colaborar para que podamos comprender qué clase de información quieren que les demos. Una de las cosas que empezamos a hacer es lo siguiente. Antes hacíamos el trabajo y publicábamos informes, informes muy técnicos que podrían ir desde 10 páginas hasta 40 páginas de extensión. Una de las cosas que empezamos a hacer es convertir esos informes en resúmenes de 500.000 palabras que puedan servir como resumen ejecutivo de lo que tratamos de decir a través de esos documentos pero sigue

estando centrado en nuestras áreas de investigación, en las cosas que nosotros pensamos que son necesidades importantes.

Quisiera invitarlos a ustedes a que hablen con nosotros. Nos encantaría trabajar directamente con ustedes pero al GAC en general quiero decirle que trabajen junto con nosotros para darnos claridad con respecto a dos cosas. Por un lado, la clase de información que les resulta útil y luego, en segundo lugar, el nivel de información. El nivel de detalle técnico que quieren. Nosotros comenzamos de forma predeterminada con un nivel técnico muy profundo. Está bien. En eso nos destacamos. Pero si ustedes quieren que subamos un par de niveles, hablen con nosotros y vamos a poder ayudarlos.

NICOLÁS CABALLERO: Muchas gracias. ¿Alguien tiene la mano levantada allí? ¿Eso quedó de antes? Tenemos que ir terminando. Nos queda un minuto. ¿Alguna pregunta o comentario final por parte del GAC? Japón, adelante.

ORADOR DESCONOCIDO: Muchas gracias por la presentación. Usted subrayó la importancia de los datos. Creo que hay distintas clases de uso indebido del DNS. No solamente la decisión de la ICANN. También hay otras formas de uso indebido. Hay otro tipo de violación de datos que se producen en Japón y en otras áreas. Creo que el problema inicial es el mismo. Quisiera saber si es necesario recopilar diferentes

clases de datos sobre uso indebido. Si hiciéramos eso podríamos colaborar con los diferentes gobiernos para obtener esa información.

RAM MOHAN: Creo que es un tema importante. Nosotros estamos preparados para trabajar junto a ustedes para darles la información técnica y el asesoramiento técnico que los podría ayudar. Creo que la solución potencial probablemente sea una combinación de la parte gubernamental, la parte técnica y la parte de políticas. Tendríamos que encontrar una forma de integrar todo eso dentro de ese foro.

NICOLÁS CABALLERO: Muchísimas gracias, Ram. Tenemos que cerrar la sesión. Gracias por sus preguntas. Ha sido una sesión fantástica, Ram, como siempre. Es un placer recibirlos aquí. Si bien para algunos estas conversaciones son un poco técnicas, tratamos de transmitir el mensaje. Ustedes hacen todo lo posible por darnos buen asesoramiento por un lado y ayudarnos a luchar contra los delincuentes. Una vez más, muchísimas gracias. Gracias, Russ. Tiene un equipo fantástico. Esperamos poder tener otra sesión en Praga. Muchísimas gracias. Un gran aplauso para nuestros amigos de SSAC.

Muchas gracias. Damos por finalizada la sesión. Comenzamos mañana a las 9:00 de la mañana, para la ceremonia inaugural y

para el otorgamiento del premio a la excelencia en la comunidad.

Muchas gracias y buenas tardes.

[FIN DE LA TRANSCRIPCIÓN]