MARRAKECH – Aspectos políticos del DNS sobre HTTPS (DoH), DNS sobre TLS (DoT) y temas relacionados
Martes, 25 de junio de 2019 – 15:15 a 16:45 WET
ICANN65 | Marrakech, Marruecos

ALEJANDRA REYNOSO: Buenas tardes a todos. Por favor tomemos asiento. Comenzaremos en un minuto. Muchas gracias.

¿Podemos preparar la presentación? Gracias. Mientras se preparar, gracias a todos por estar aquí. Vamos a tener una sesión sobre un tema de alto interés que es sobre el DNS sobre HTTPS y sobre el TLS. Primero la agenda será la siguiente. Yo les voy a introducir, primero, cuáles son los objetivos de esta sesión, voy a presentar a nuestros panelistas.

Habrá una reseña técnica sobre el tema. Luego tendremos una sesión de preguntas y respuestas y después las preocupaciones posibles a la hora de la implementación o despliegue, otra sesión de preguntas y respuestas y al final un panel de discusión y consideraciones primarias. Esperamos la participación de todos ustedes en este tema de alto interés. Tendremos micrófonos volantes. Les pedimos que nos digan dónde están. Tenemos números para identificar a los micrófonos. Veo el cuatro, el seis, ahí están los micrófonos.

Entonces, cuando tengan una pregunta, por favor, levanten la mano lo más alto posible para que los asistentes se acerquen y le entreguen el micrófono.

Sería fantástico tener la presentación. Comenzaré presentándome. Yo soy Alejandra Reynoso del ccTLD de .GT. Conmigo está Danny McPherson. Danny es el Vicepresidente Ejecutivo y Director de Seguridad de Verisign, es miembro de SSAC también.

También está Peter Koch. Peter trabaja por el administrador del ccTLD de .de actualmente como asesor en políticas. También tenemos a Barry Leiba. Barry es Administrador de Normas Estándar en Futurewei Technologies. Barry ha trabajado en tecnologías de correo electrónico y otras desde finales de los 80 y trabaja actualmente en internet de las cosas; mensajería y colaboración en plataformas móviles, seguridad y privacidad de la internet y estándares en su desarrollo y despliegue para la internet. También es miembro del SSAC.

Tendremos a Alyssa Moore. Ahí está. Pido disculpas por no marcar dónde están las personas. Alyssa es asesor de política de CIRA que es la autoridad de .ca sobre la administración del ccTLD .ca.

Ella moderará las preguntas y el resto de los panelistas son Tim April. Tim es Arquitecto de Seguridad Principal en Akamai Technologies. Trabaja en Networking DNS en respuesta ante incidentes. Tim también es miembro del SSAC.

¿Podemos avanzar un par de diapositivas, por favor? Y también estará Vittorio Bertola. Vittorio Bertola es el Jefe de Política e Innovaciones de Open-Xchange, la compañía matriz de PowerDNS que ha venido discutiendo las consecuencias de la interferencia de DNS en varios foros durante el último año.

Y, por último, tenemos a Michele Neylon. Michele es Fundador y CEO de Blacknight Solutions que es un registrador acreditado. También es miembro del consejo de la GNSO.

Avanzamos un par de diapositivas. Parece ser que tenemos como siempre algunas cuestiones técnicas, pero no es anda difícil. No sé si comenzar con la reseña técnica sin tener las diapositivas. ¿Podemos? Por el tiempo.

Vamos a esperar un minuto más a ver si se muestran las diapositivas, si no, comenzamos. Un par de segundos. Mientras tanto pueden ir descargando las diapositivas de la agenda, así podemos comenzar nuestra conversación. Danny, si le parece.

DANNY MCPHERSON: Por supuesto, voy a comenzar sin las diapositivas. Es suficientemente difícil este tema con las diapositivas, así que imagínense. Yo soy Danny McPherson, miembro del SSAC y ahora voy a presentar las diapositivas que tienen que ver con el SSAC, con los errores o los aciertos que tuvo el SSAC.

Voy a hablar de lo técnico y Peter y Barry van a hablar de las implicancias políticas. El tema general ha adquirido mucho interés reciente por lo que se llama DoH y DoT, que es DNS sobre HTTPS y DNS sobre TLS.

En esencia, estas tecnologías proporcionan confianza en las transacciones en la internet. Por tradición, DNS tenía incorporada la noción de confidencialidad, no la de integridad, peor DNSSEC lo complementó para dar protección e integridad al DNS. Pero todavía está viendo el DNS cuestiones tales como vigilancia, eavesdropping, escuchas y por varias razones tales como control de velocidad, censura estatal, bloqueo de acceso a sitios maliciosos, todo para proteger al usuario.

Hay muchos motivadores por los cuales tenemos esa ruptura. Pasemos a la diapositiva 6 donde van a ver varias de las razones por las cuales es así. El DNS tradicional tenía esta noción de confidencialidad entonces. El estado actual Geopolítico en el que vivimos con las consecuencias económicas, tener

confidencialidad en las transacciones en el DNS tiene beneficios. Vamos a hablar de estos modelos.

La diapositiva 6 habla, básicamente, de lo que estamos cubriendo sin confidencialidad de las transacciones, la información está disponible para que otros sepan a dónde vamos. Y pueden hacer minerías de información.

La noción entonces de DoH y DoT es dar protección para que los atacantes, los hackers no vean esa información. Eso es, básicamente, de lo que estamos hablando cuando hablamos de DoH y DoT. En la diapositiva 7 explica lo que es el DNS tradicional. En el DNS, básicamente, tenemos un dispositivo y por dispositivo me refiero a una aplicación que quiere resolver algo en el DNS y le pide al procesador local, por ejemplo, al browser, le puede pedir al iPhone o a la computadora, cómo llegar al, por ejemplo, www.example.com.

El DNS tiene un resolutor que habla con la red local o con la red del ISP, entonces, ¿podremos avanzar dos diapositivas más? A la imagen que habla del DNS tradicional. Esto es lo que estaba explicando hace un instante. Tenemos las aplicaciones que quieren resolver algo para el usuario o el proceso del dispositivo, la aplicación se contacta con el sistema operativo local que puede ser de la aplicación del iPhone o un navegador web en la laptop y esa aplicación, ese browser, le pregunta al sistema

operativo dónde está ese nombre de destino en la internet y ese dispositivo sale a comunicarse, ya sea con lo que se llama forwarder local o un resolutor recursivo.

Tradicionalmente los resolutores recursivos es el que tiene el ISP en la red local, pero cada vez es más común que esté en una infraestructura de nube, por ejemplo, un DNS abierto, algo que está en la infraestructura de la nube. Esa es una de las diferencias arquitectónicas principales. Puede no estar en la red tradicional y ese servidor de nombres recursivos va a la estructura autoritativa, la infraestructura del TLD y resuelve el nombre y pasa la información de vuelta a la aplicación o a resolutor mínimo o stub que se la devuelve a la aplicación y la aplicación ahí se puede conectar con el destino en internet que desea.

Como ven, en este diagrama todas esas transacciones no tienen esa noción de confidencialidad de transacción incorporada. Para un observador, cualquiera de esos caminos donde hay una flecha verde, podría el observador ver qué está pasando. Puede ser información de naturaleza competitiva comercial, pueden ser contenidos ilícitos, lo que sea.

Aquí entonces con DoH y DoT estamos hablando de maneras de proteger esa información. Entonces, una de las dos soluciones es lo que se llama DoT. DoT es DNS sobre TLS, TLS es lo que llamamos la Transport Layer Security, la Seguridad de la Capa de

Transporte. La mayoría de las transacciones en la internet en un padlock típico de un sitio financiero donde se guarda la información, la TLS es el protocolo que soporta todo, da encriptación a nivel de la red, o sea, confidencialidad de la información.

Entonces, si un atacante quiere entrar a manipular o a observar la información es prevenido. En el modelo DoT, pasemos a la siguiente diapositiva. En el modelo DoT, ¿qué pasa? El DNS sobre TLS puede desplegarse según distintas técnicas, está todo en el protocolo en la comunidad operativa. DNS sobre TLS tiene esta visión, un sistema local, por ejemplo, el iPhone, la laptop, pueden tener una configuración para todo el sistema que diga, “voy a usar este resolutor para resolver cosas en el DNS”.

Y todas las aplicaciones para hacer alguna resolución tienen que ir ahí, por ejemplo, un navegador web que hace lo mismo que hacía siempre, le pregunta al resolutor mínimo, por ejemplo, en el www.example.com dónde lo hago. El resolutor en vez de enviar un texto no encriptado, lo envía por un canal encriptado, ya sea un forward o algún otro tipo de infraestructura o a la red del ISP para resolverlo y eso es lo que vemos en las flechas rojas.

O sea, para un observador de la trayectoria, ve esa información encriptada y después más adelante en la infraestructura, la del servidor autoritativo, ahí no hay mucha consideración hoy día

sobre cómo las soluciones DoT o DoH podrían incorporarse ya sea en la infraestructura del segundo nivel pero va a venir.

En un momento esto lo vamos a comparar con DoH que, básicamente, pasa el nivel de encriptación para atrás. Y pasemos más adelante a hablar de DoH. Estoy muy rápido, hablando muy rápido, perdón.

Entonces, básicamente, al definir TLS para el transporte en el DNS, ¿qué pasa? Hay muchas aplicaciones en el dispositivo o mucho tráfico en la web o mucho software, entonces cada transacción en este sistema operativo del dispositivo en lugar de usar TLS nativamente en la infraestructura, codifica las respuestas del DNS en las consultas del DNS y lo pone sobre la TLS, que es donde corre el HTTPS y luego pasa a la red.

Entonces hay muchos espacios o muchos lugares donde la aplicación puede transaccionar directamente con la red y pasar por alto al resolutor mínimo o usarlo desde el sistema operativo. Les voy a dar un ejemplo. Este es un modelo de despliegue y hay distintos. ¿Qué puede pasar? El navegador puede usar un servidor de nombres recursivo con DoH en la infraestructura, mientras que otra aplicación puede usar uno local o puede ser el resolutor del sistema. Lo interesante es que si algo se rompe en este escenario, distintas aplicaciones usan distintas DNS, esto puede complicar lo que vemos.

Otra cosa que pasa es que los ISP tradicionalmente pueden usar consultas como punto de control en la infraestructura o la organización puede usarlo, y a lo mejor, no quieren tener transacciones encriptadas que vengan de una aplicación en algún punto de frontera porque lo hacen como una garantía de seguridad o para cualquier otro tipo de control.

Entonces, aquí en lugar de usar el resolutor stub, en el caso de DoH, es un planteo más tradicional. La aplicación va a consultar directamente a la infraestructura de resolución de la internet para tener la respuesta y pasa por alto todo lo demás. Lo hace a través, posiblemente, de un proveedor de servicios de internet local y de ahí sigue como siempre.

Otra cosa interesante a señalar. Si esto lo vemos desde la perspectiva de la vigilancia, la escucha o el control, el DoH como ven se combina con el tráfico de resolución, con el otro tráfico HTTPS, se mezcla, entonces es mucho más difícil hacer filtros o seguimiento o vigilancia. Habría que abrir todo ese tráfico para hacer algo, técnicamente desde el punto de vista de control con resoluciones del DNS del tipo DoH. También podría hacerse a través de toll sistema, es posible.

Y otra cosa que muestra esta diapositiva es que el modelo de despliegue que vemos tanto para DoT como DoH pueden ser combinados y esas flechas pueden ser invertidas o mezcladas.

Dependerá de lo que habilite o no el administrador. Entonces un sistema, como un sistema operativo mínimo, preferiría usar DoH en lugar de DoT o DNS tradicional. Todavía se está definiendo. Todavía no se ha pensado demasiado sobre la infraestructura autoritativa, root, .com, edu, Jobs. No sé, no importa cuál sea el TLD o incluso posiblemente de segundo nivel hay otras técnicas como minimización QNAME que da privacidad de protección. Al igual que hay que hacer concesiones con otros aspectos también.

Bueno, creo que he intentado cubrir todo, sé que hablé muy rápido, pero vamos a hacer aquí una pausa a ver si tienen preguntas antes de pasar a Peter quien hablará sobre las consideraciones del despliegue. Quería saber si tienen alguna pregunta para el panel o pueden tomar nota de ellas y permitir que Peter hable sobre otras aplicaciones de DoT y DoH y después hacer las preguntas.

ALEJANDRA REYNOSO: Gracias, Danny, por esa presentación tan rápida. Y aquí tenemos una pregunta. Muchas gracias.

NIGEL CASSIMIRE: Buenas tardes, soy Nigel Cassimire de la Unión de Telecomunicaciones del Caribe. Esto para mí es nuevo, estoy tratando de entender el problema que queremos resolver con

todo esto. ¿Es esto un intento para que el DNS sea más seguro? ¿Y cómo se compara esta técnica con, por ejemplo, DNSSEC?

MICHELE NEYLON: Ahora estamos peleándonos a ver quién responde. Yo voy a hablar. DNSSEC es un tema del que se habla mucho en los círculos de la ICANN como la solución mágica para resolver todos los problemas del DNS, pero no es así. DNSSEC es una manera de decir… Bueno, cuando vamos al sitio de banco. El que fuere y alguien ha insertado algo en el medio, ese tipo de ataque es lo que se llama envenenamiento del DNS que ha sido una cuestión en algunos lugares en el pasado y DNS eso lo resuelva.

Con DoT y DoH lo que se intenta es tanto añadir un nivel más de privacidad como de seguridad, pero hay en ambos casos problemas. La privacidad sí se pasa por alto, probablemente hablaremos un poquito más sobre esto después, cuáles serían las implicancias negativas en lo que hace a la seguridad. Pero lo que hace en esencia es, pasar esas queries del DNS de la misma manera que hacen los lookups de las búsquedas de los dispositivos como se hace en el teléfono, en el iPad. O sea, se las quita del DNS tradicional y se las pasa, se las pone a cuestas de otros protocolos.

En el caso del DoH se ve como una solicitud web tradicional. No soy tan técnico yo como él, seguramente me va a corregir, pero es una manera sencilla de ver la cuestión.

ALEJANDRA REYNOSO: Gracias, Michele. Tenemos un participante remoto. Adelante.

ARIEL LIANG: Hay dos participantes remotos que han hecho preguntas. La primera es de Mohammed Yousif que pregunta si el DNS sobre DoH genera una degradación en la performance en cuanto a la resolución de una consulta. Y ahora voy a la segunda pregunta. No, perdón, la voy a leer después.

MICHELE NEYLON: Depende de cómo se implementa el resolutor stub. Puede imponer al resolutor una conexión inicial, pero si ese stub está configurado para persistir. Con el tiempo el costo puede ser el mismo que el del DNS.

ARIEL LIANG: Hay una segunda pregunta que es de Yazid de Benin que dice: Las tecnologías como la administración del QNAME podrían ser

efectivas en preservar la privacidad del usuario. ¿Cómo se puede implementar esto en todos los resolutores?

DANNY MCPHERSON: No queríamos hablar mucho sobre la minimización del QNAME, pero es una técnica bastante leve. Tradicionalmente DNS es robusto y si yo quiero resolver algo en DNS, doy un dominio calificado, un servidor interno secreto como Verisign.com y le pido a todo servidor autorizado, le pregunto la misma cosa, le hago la misma pregunta y lo único que tengo que saber es cómo llegar al próximo nivel de jerarquía que es el .com.

Yo no digo todo lo que tengo que decir, sino cómo llegar al .com y en .com veo cómo llegar a Verising.com y Verisign.com me dice cómo entrar al servidor secreto. Es decir, que no divulgamos el nombre entero y así minimizamos la privacidad en la función de resolución de nombre. Es muy liviano y se implementa con mucha facilidad, ya está implementado en muchos servidores recursivos en distintas formas da minimización de ataques desde una perspectiva de seguridad.

ALEJANDRA REYNOSO: Le voy a pedir a todos que se mantengan en el tema. Sabemos que hay conceptos muy vinculados a la seguridad de internet, pero ahora quisiéramos centrarnos en DoT y en DoH para que los

panelistas puedan continuar. Voy a tomar dos preguntas, el número 4 y el número 5 y luego pasamos al siguiente presentador. Gracias.

FRED BAKER: Me sorprendió su respuesta sobre la diferencia entre TLS y correr DNSSEC porque aseguran dos cosas distintas. DNSSEC asegura el contenido, la estructura del recurso, mientras que TLS asegura el canal. Por comparación podemos pensar en términos de, por ejemplo, imaginar que tengo el mejor caño del mundo y tengo un lago que está lleno de veneno y cuando se transporta a través de ese excelente caño, sigue transportando veneno.

Asegurar el contenido nos evita el tema del veneno. No voy a hablar de TLS porque tener un buen canal es algo bueno, pero DNSSEC es muy importante en términos de garantizar que el nombre lleva lo que estamos pensando que debemos lograr.

DANNY MCPHERSON: Voy a responder. Es un buen punto. Incluso si tenemos DoH o DoT completamente desplegado en el ecosistema, igual hay que tener minimización de DNSSEC porque tratan dos cosas muy diferentes.

ALEJANDRA REYNOSO: ¿Número 5?

JIM PRENDERGAST: No soy una persona de IETF. Sé que hay muchos de ustedes aquí en la sala que lo son. Danny, cuando hablabas de los beneficios también decías que hay cosas que pueden dejar de funcionar. ¿Cómo se aprobaría esto como estándar si hay cosas que tienen consecuencias no intencionadas, incluso ahora que están ocurriendo?

ORADOR NO IDENTIFICADO: Es una buena pregunta

DANNY MCPHERSON: Creo que la tecnología está, el ecosistema se va a adaptar para ver cuál es el mejor modelo de implementación. No creo que nadie en el ecosistema, ni en los sistemas operativos, ni en los operadores de servidores recursivos quieran que algo no funcione. Esto causa desafíos en la implementación, de todos modos. Si soy un ISP y no tengo visibilidad para el tráfico de usuarios en DNS y tengo que resolverlo con otra forma de DNSI y causar un problema, quizás no podamos hacerlo. O si implementamos control parental en DNS, quizás no lo podamos hacer.

El ecosistema va a tener que ajustarse a eso y por eso me parece a mí que es tan importante para DoH como para DoT ver que los modelos de implementación van a ser adaptivos y se van a acomodar a la mejor dinámica que funcione mejor.

ALEJANDRA REYNOSO: Gracias. En resumen, ahora vamos a escuchar sobre los acontecimientos potenciales.

PETER KOCH: Hola. Gracias. Soy Peter Koch, soy Asesor Senior y uno de los co-conspiradores designados por la ccNSO en este grupo.

Me invitaron para hablar sobre las preocupaciones potenciales y el título no oficial es que el protocolo se implemente y luego ocurran cosas. Esto es lo que seguramente va a tratar alguna de las inquietudes. Lo primero es lo técnico, tenemos dos estándares que tratan.

ALEJANDRA REYNOSO: Otra diapositiva, por favor.

PETER KOCH: Esta es. La voy a hacer entonces a partir de aquí. Tenemos dos estándares que se ocupan del mismo tema de la confidencialidad

del tráfico de DNS que va y viene. Y les quiero recordar por qué. Hubo una persona que se llama Snowden, hace algunos años y se descubrió que el tráfico del DNS puede ser una fuente de inteligencia y que se puede utilizar para identificar a personas o para identificar acciones en las que se ocupan las personas como sitio web.

Pero no nos ocupemos ahora en los sitios web para los que se usa el DNS, sino los otros servicios también. Ese es uno de los factores sobre los cuales tenemos documentos publicados. El IETF declara que es una amenaza que se debe mitigar por un par de protocolos. Estos intentos, en realidad, están abordando este tema al responder al monitoreo invasivo con una encripción, es decir, que es encriptar el tráfico de DNS y hay otros aspectos técnicos también.

Pero para agregar. Son también otras las piezas en el rompecabezas que pueden ver el tráfico del DNS que va y que viene. La información en el DNS es pública, pero el hecho de que alguien pide un nombre o un número específico en el tiempo posiblemente no sea público y es información válida.

Dicho esto, tenemos dos estándares que compiten y es bastante fácil de describir. Una parte, el resolutor se comunica con la otra parte que, en este caso, es el resolutor DoH. Es como un servidor web desde afuera, pero en vez de entregar websites, entrega

respuestas de DNS. Lo que no está resuelto hasta ahora es de qué manera el usuario, el navegador en este caso, recibe la información que se solicita. Normalmente esta es una información que es entregada por el sistema operativo en esos casos en los que lo tenemos que es el caso de una computadora o un teléfono.

Hay una resolución de nombre que está muy incluida en el sistema operativo. Hoy en día esto se hace consistentemente en toda la caja que ustedes tienen frente a ustedes, o en la mesa, y esto podría cambiar. La idea para los desarrolladores es trabajar en la configuración automática, cómo encontrar este resolutor y también hay iniciativas en marcha para que los usuarios tengan más elección y que puedan configurar manualmente los servidores de DNS. Pero esto todavía se está preparando.

Ya hubo un proveedor para el cual se permitió el DNS sobre HTTP, es decir, tratar la resolución de DNS un poco como ocurre en la web y esto tiene un url con código duro, este sirve de identificador que ustedes seguramente conocen a partir del servidor web cuando ustedes visitan página web y esa información entra en el DNS.

Es decir, que el proveedor habría utilizado un resolutor DoH en particular, es decir, que no habría sido una instancia única, aienicas y todo eso y esto pasaría por encima. La información que

está siendo entregada por el sistema operativo. Es decir, que la aplicación ahora podría elegir un camino de resolución de DNS diferente a lo que hace el resto del sistema operativo. Esto puede tener algunos desafíos y puede también interferir en algunos gestores de red que tienen políticas de seguridad donde se trata de mitigar cierta información, fundamentalmente sitios de phishing al interceptar el tráfico de DNS. Y como aquí ya se ha dicho, podría presentar un problema.

La pregunta interesante es: ¿Por qué hay dos estándares entonces? Estoy tratando de no entrar a la cuestión técnica, pero DNS sobre la capa de seguridad de transporte quizás tiene algo que ver más con la ingeniería, hablamos de distintas capas, etcétera, pero tiene al menos un problema que es que se necesita otro agujero en el firewall para acceder a la información, y aquí todo el mundo le está permitiendo a todo el mundo entrar en su servidor web.

El tráfico DoH se ve un poco más como el acceso a un sitio web no se puede separar como vamos a ver en la próxima diapositiva o en esta, en realidad. Es decir, que no se puede bloquear el acceso al servicio de resolución de nombres con DoH sin bloquear el acceso a los servicios web importantes. Este es el truco. Y todavía se están haciendo investigaciones para agregar esta

característica al DNS sobre el TLS como el enfoque DoT. Hay algunos otros detalles que no son parte del tema de hoy.

Como consecuencia de los gestores de red, quizás no puedan bloquear la resolución de nombres. Esto se debe a que al mismo tiempo ellos podrían bloquear el acceso a los sitios web o a los motores de búsqueda populares. Esto puede o no interferir con algunos requisitos regulatorios, en algunas jurisdicciones donde los ISP reciben órdenes de bloquear la resolución de ciertos nombres de dominio y aquí no estoy diciendo que estos mecanismos de bloqueo sean muy efectivos, pero puede haber cuestiones regulatorias.

Como dije, nunca puede ser perfecto porque se puede circunvalar al configurar el propio resolutor utilizando un VPN o corriendo el propio resolutor en el propio sistema. Al poner más caras en el tráfico web, se podría ayudar a los usuarios al llegar al DNS. Eso ocurre que cuando hay una censura y también cuando se bloquea el malware que puede ser que se refiera a legislación que se adopta en interés del usuario.

Vamos a ver un poco el panorama general. El protocolo es donde ocurren cosas raras. DNS sobre HTTP no prescribe ningún modelo de implementación en particular. Cualquier empresa puede correr un resolutor DoH y dirigir el sitio hacia allí. Sin embargo, en las discusiones hasta ahora, podemos observar un modelo que se

vincula a la concentración y la consolidación como en los proveedores de servicios web que cooperan con los proveedores de resolución de DNS. Voy a hablar de eso en el punto siguiente.

Los web browsers cooperan con los resolutores y todos los clientes tienen usuarios web que los llevan a la resolución de servicios de un proveedor en particular, lo cual le da al proveedor un gran conocimiento, un poco de estabilidad para los usuarios, pero genera concentración.

La resolución de nombres de DNS tradicionalmente donde los últimos 38 años era muy descentralizada, es decir, que los ISP, o incluso en una laptop, si no pensaba hace 30 años o en una mainframe o lo que fuere. La resolución de nombres de DNS como servicio, evolucionó a lo largo del tiempo y estos son los que se llaman quads como 1.1.1.1, 8.8.8.8. Ustedes seguramente lo ven pintado esto en una pared en países donde la gente tiene bloqueos de DNS y lo circunvalan al ir a través de uno de estos proveedores de resolución. Utilizan el mismo número en la misma posición, es una cuestión de seguridad.

Estos aspectos además de la elección del camino de resolución por aplicación y no por sistema o por empresa, o incluso por ISP donde el ISP da la resolución al cliente, definitivamente lleva a una concentración aumentada de los resolutores que cada vez son más grandes. Y con grandes queremos decir que la población

detrás de ese resolutor crece, crece, crece y obviamente el peso, y eso también podría implicar el peso de política de ese resolutor u operador se puede esperar que va a crecer y va a ser cada vez más importante.

Como dijimos, DoH y DoT ambos proveen privacidad en el cable y lo dijimos por varias razones. Los resolutores y hay incluso resolutores en el ISP o resolutores que están ofrecidos por estos grandes servicios de resolución, sí ven los pedidos de los usuarios y tienen distintos niveles de detalle. Por alguna razón, muchas veces hay información en particular que se agrega a las preguntas y los usuarios pueden tener respuestas específicas porque como vemos en el último punto, algunos escenarios técnicos depende del hecho de que no todo el mundo recibe la misma respuesta cuando hace la misma pregunta.

Hay redes de entrega de contenido que llevan a los usuarios al sistema de contenido más cercano para bajar la latencia y darles a los usuarios la respuesta. La privacidad no solamente se aborda a través de la encriptación en el cable, sino también a través de la política de resolución como en los operadores de resolución que les prometen que van a ser responsables sobre los datos que pueden haber circunvalado el ISP o el actor que podría estar interesado en los datos pero que no tiene mucha idea si es que incluso el resolutor está operando allí.

Entonces, preguntas de política para los resolutores DoH. Esto es algo para discutir. ¿Cómo se deben seleccionar? Vamos a ver cómo yo como usuario decido cuál usar y si me decidí por uno o por otro como lo configuro en mi aplicación, en mi sistema o que. Y que los operadores de estos resolutores de DoH cómo son responsables por lo que prometen y por lo que hacen porque nuevamente puede requerirse que divulguen información a través del período de una entidad en general la aplicación de la ley.

¿Y quién determina cuáles son las políticas que son aceptables? Como dijo un proveedor, okay, nosotros entendemos que hay preocupaciones en la comunidad de que hay algunos proveedores con lo que cooperamos y nosotros entonces estamos abiertos a cooperar con otro, pero quisiéramos tener o quisiéramos, mejor dicho, que ellos se adhieran a ciertas políticas de resolutor y eso significa que ellos hagan y no hagan ciertas cosas con los usuarios.

Entonces, vamos al panorama incluso más amplio porque alguna de las preguntas va a ser por qué estamos hablando de esto en el contexto de la ICANN. Supongamos que un grupo coopera con los proveedores de resolución, el grupo va a ser pequeño, no va a ser tan extendido como ocurría antes y asomamos incluso que hay ciertas aplicaciones o servicios que se utilizan en forma

dominante en internet como la web, como todos hacemos y a veces hay un interés en los caminos de resolución adicionales.

Hubo una discusión en el IETF y también en la ICANN sobre punto en un TLD, pero se trata de un camino de resolución diferente y que se necesita apara algo que de alguna manera encaja en el espacio de nombre.

Hablando de modo práctico, con este grupo de proveedores de resolución de servicios tenemos una población que está por detrás de ellos que realmente estaría en una posición de decidir si se debe abrir un nuevo segmento del espacio de nombre o no. ¿Y eso cómo se vería? ¿Qué implicaría esto para el rol de la ICANN respecto a la zona raíz del DNS cuando existe un cambio en el poder donde hay simplemente que votan con sus pies?

Conclusiones. Conclusiones preliminares, probablemente. Hemos aprendido que parte de la implementación del DoH y el DoT podría impactar en los puntos de control tradicionales en la resolución. Los ISP y el Enterprise pueden interceptar consultas de DNS y enviar distintas respuestas para mitigar malware y botnets.

La estandarización del DoH y del DoT o de los resolutores en las aplicaciones y en cómo se seleccionan todavía está en marcha. No hay ninguna conclusión final. Para los registros, los

operadores de registro y los registradores pareciera que actualmente hay poco impacto. Sin embargo, podría haber alguien que le toca la puerta a los registros o los registradores y que dice: Yo soy uno de estos proveedores de resolución, ¿por qué no me das una copia de los datos de DNS? Estoy muy interesado en entregarles esto a tus usuarios.

Y, por supuesto, es muy temprano decir cuál va a ser el impacto a los usuarios. Como ya escuchamos, esto afecta a otros mecanismos y la necesidad no ha cambiado y eso debería ser todo. Siguiente diapositiva.

ALEJANDRA REYNOSO: Muchas gracias, Peter. ¿Alguna pregunta del público? Tenemos tiempo para un par de preguntas. Tengo el número 5.

WARREN KUMARI: Trabajo para Google. Peter, en su presentación usted mostró un modelo de despliegue de uno de los navegadores, pero no es el único nivel de despliegue. Chrome lo que planea hacer es ofrecer DoT a los usuarios de dos maneras. Si el resolutor del sistema del usuario ya soporta DoH, Chrome básicamente hará una actualización para usarlo. Entonces, si usan los resolutores del ISP y soporta DoH, Chrome se va a actualizar.

Si el usuario quiere, puede usar un resolutor distinto, que es básicamente lo que está pasando ahora. El usuario en el resolutor del ISP puede usar otro. Más allá de eso, Chrome no va a cambiar lo que el usuario haya seleccionado sin darle la opción expresa. ¿Todo esto que significa? Significa que las protecciones actuales que la gente tiene para cosas como malware si hacen DNS técnico a nivel empresarial, bueno todo eso va a seguir funcionando igual.

Lo que quiero decir, es que lo importante es la forma en que esto se instale, no cuál es el transporte. No sé si tiene algún comentario al respecto.

PETER KOCH: Sí, gracias Warren. Deliberadamente no puse nombres en esta diapositiva, espero no haber mencionado a nadie, pero gracias a usted por haberlo mencionado.

En este caso particular sí es una visión valiosa. El modelo no procuraba ser exhaustivo, creo que las diapositivas decían que se están discutiendo múltiples modelos y el que usted nos indicó, obviamente es uno de ellos. Con respecto al resto, me gustaría diferir esto hasta el panel posterior a ver si nos podemos concentrar ahora en preguntas inmediatas sobre cosas que no hayan compartido.

ALEJANDRA REYNOSO: Tenemos un participante remoto y después el micrófono 3 y terminamos la lista de preguntas para esta parte.

ARIEL LIANG: Hay una pregunta de Dirk Jumpertz. El DoH ya ha sido abusado como vector de ataque para insertar contenidos maliciosos en páginas web a través del uso de registros TXT falsos. ¿Conoce esto? Es muy difícil de bloquear ya que el canal es un canal de confianza del usuario. Combinando DNS con THT, ¿esto hace que esto se convierta más en una amenaza que una bendición?

PETER KOCH: Interesante información. La verdad es que yo no la conocía. Quizás los panelistas, por eso me gustaría diferirlo a la sesión del panel y yo lo voy a recordar.

ALEJANDRA REYNOSO: Número 3.

EDUARDO DÍAZ: Habla Eduardo Díaz, Presidente de NARALO. Tengo una pregunta. Un posible problema para el usuario es: Si yo descargo una aplicación que usa sus propios resolutores en la descarga. ¿Eso

podría afectar muy rápidamente al usuario que no sabe qué está pasando detrás?

PETER KOCH: Sí. Gracias por ese comentario. Un aspecto que no mencioné, es que en teoría, que después se convierte en la práctica, las distintas aplicaciones pueden dar distintos resultados. El sistema de nombres de dominio se ve distinto desde lo que es un navegador o una aplicación de mail o un teléfono porque dependiendo del camino de resolución, algunos nombres de dominio pueden estar bloqueados y otros no, o llegar al mismo punto A desde distintos caminos. Eso una diferente experiencia del usuario. Gracias.

ALEJANDRA REYNOSO: Número 4.

REMMY NWEKE: Gracias. Yo soy Remmy de Nigeria. Represento a la Unidad Constitutiva de Partes No Comerciales. Mi preocupación tiene que ver con uno de los comentarios de la diapositiva que es demasiado temprano para decir cuál será el impacto de DoH o DoT sobre los usuarios, pero al menos podemos intentar analizar el impacto negativo sobre el usuario. Una aclaración le pido.

¿Cuáles son las contramedidas que podríamos usar para contrarrestar este impacto negativo del DoH y el DoT? Y también, ¿cuáles son las responsabilidades para el usuario? ¿Cuáles son las implicancias en términos de costos y comunicación? Gracias.

PETER KOCH: Creo que esto más que una pregunta ha sido un aporte que podríamos incorporar a la discusión. Tenemos dos diapositivas más antes de abrir el panel, así que no veo que haya más preguntas.

ALEJANDRA REYNOSO: No, pasamos al panel ahora. Avanzamos un par de diapositivas. Muchas gracias. Ahora los panelistas responderán estas preguntas. Las voy a leer.

¿Se prevé algún impacto del despliegue del DoH o DoT en sus operaciones?

¿Hay alguna cuestión con DoH o DoT que le corresponda o que esté dentro de la misión de la ICANN?

¿Cómo piensa usted que e DoH se implementará en aplicaciones como los browsers de web?

¿Qué preocupaciones tiene sobre el DoH y el DoT? Así que vamos a comenzar con Tim.

TIM APRIL: Me llevaría la vida contestar todas estas preguntas, pero como soy una persona técnica, lo que surge básicamente respecto de las preocupaciones, tiene que ver, en general, con los usuarios finales y con su percepción del espacio de nombres como puede cambiar. Si la primera milla desde el browser, desde la aplicación hasta el resolutor usa DoH o DoT, la privacidad del canal reside ahí, pero eso no es garantía de que la conexión desde ese resolutor hasta el autoritativo tenga protección.

Si les preocupa la fuga de información a través de ese canal de comunicaciones, eso puede ocurrir después del resolutor. Y en algunos casos, puede ser incluso atribuido al mismo usuario. También hay un problema de debugging. Dependiendo de la implementación que se elija, específicamente en DoH, si la aplicación usa un resolutor DoH sin conocimiento, puede haber algún tipo de problemas de resolución que el usuario puede asignar al ISP o a otra cuestión y genera todo un proceso de debugging y eso afecta al usuario que es mayor el impacto cuanto menos conocimiento técnico tiene.

ALEJANDRA REYNOSO: De acuerdo. ¿Vittorio?

VITTORIO BERTOLA: Varias cosas. La primera pregunta. Yo he sido proveedor de software y los ISP tienen un impacto en el despliegue en el mundo real. Nos preocupa, como compañía de software de código abierto, el impacto que esto puede tener en la forma del mercado del DNS como mercado de resolución. Aquí la cuestión no tiene que ver tanto con la encriptación, el tránsito y la recopilación de la información, sino la remoción del DNS. Pasar de un servicio de red algo que se proporciona más allá de cuál sea el proveedor de servicios de internet o el sistema operativo como HTTP stack a pasar a una aplicación. Y esto abre el panorama a muchos problemas que tiene que ver con confusiones posibles, como dijimos, que las distintas aplicaciones sigan distintos caminos.

La más preocupante es que el mercado de las aplicaciones ahora está mucho más concentrado en el mercado de la red. Actualmente si uno quiere, el 95% de las queries del DNS apuntan a los 1,000 resolutores más importantes que manejan algunas compañías, que están todas, de paso lo digo, en el mismo país, en la misma jurisdicción.

Entonces, en lo que hace el tema de soberanía y jurisdicción, esto va a cambiar muchas cosas porque todos sabemos que para los

gobiernos… bueno, muchas unidades constitutivas se verán afectadas como los ISP, pero creo que estamos hablando aquí de los gobiernos y los usuarios finales. Para los gobiernos el impacto es saber quién está, quién tiene el control de la resolución del DNS. Por ejemplo, en especial para aquellos proveedores que dan servicios adicionales como control parental. Así los browsers se convertirán en plataformas globales y todo el control pasará a manos de ellos y dejará de lado la jurisdicción del país.

Por eso, el Gobierno Británico ha prestado atención a esto y varios otros también. Para los usuarios es un impacto en lo que hace la elección porque si la aplicación decide enviar las consultas a donde quiere, se limitan las elecciones.

Uno de los despliegues habla de quiénes manejan los resolutores. Como decía, tenemos algunos poquitos resolutores que lo permiten. Se convierten en los porteros, están a cargo de la llave de entrar. O sea, depende de la política y este es mi último mensaje. Depende del modelo de despliegue y hay que tener algún tipo de política compartida para que la gente de las aplicaciones haga lo que quiera y que todo se entienda.

ALEJANDRA REYNOSO: Gracias, Vittorio. Michele.

MICHELE NEYLON: Las preguntas que leemos aquí no son para nada sencillas. Son muy difíciles las que me gustan. Algunos de estos temas todavía son muy teóricos y académicos. Es muy temprano todavía. DoH, DoT hasta hace muy poquito eran hipotéticos y ahora son una realidad, ¿y cuál es esa realidad? ¿Cómo va a impactar esto? Y voy a la segunda pregunta.

La misión de la ICANN podría verse afectada de alguna manera. Si terminamos en una situación en la cual los identificadores únicos ya no sean más públicos donde tengamos un número mucho más reducido de operadores de resolutores que deciden qué va sobre el DNS, o sea, qué es lo que la gente puede visitar, qué sitios llegar. Ese podría ser un impacto potencial.

Mi compañía es un proveedor de alojamiento, un registrador y también brindamos servicios de ISP. La gente no entiende qué es un nombre de dominio, no entienden la diferencia entre un nombre de dominio y un browser, ni la diferencia entre motor de búsqueda y una barra de un navegador, de un browser. Entonces, cuando uno dice, “ah bueno el usuario puede elegir qué servicio usar”. Eso puede ser verdad con los fanáticos de la tecnología, pero ¿cuántos de los presentes manejan sus propios servidores de nombres? ¿Y cuántos de ustedes…? Okay, okay, veo la sala y sé que son todos los fanáticos los que están aquí, los únicos.

¿Cuántos de ustedes administran su propio servidor de correo electrónico? De paso, es la misma gente en su mayor parte.

¿Alguno de ustedes—? Sean honestos, pongan la mano en el corazón, ¿—dirían que son un usuario típico de internet? Y esa es la cuestión. Decir que hay opción, elección, no es una verdad total. En definitiva, los aspectos de política técnico, esto es como abrir la caja de pandora en muchos aspectos.

Si vemos en la presentación de Danny, él hizo comparaciones entre las distintas tecnologías. La pregunta es preguntarnos por qué esto ocurre, de dónde vino todo esto y la realidad es que en el mundo en el que vivimos hoy, la privacidad y la seguridad son las cosas que a la gente le preocupa. Si no les preocupa a ustedes la privacidad y la seguridad, ¿dónde han estado los últimos años? El DNS en muchos aspectos fue demasiado público. Tenía muchas cuestiones interesantes y ahora tenemos una posible alternativa para resolver algunos de estos problemas que abre una serie de nuevos problemas que, por supuesto, va a hacer que muchos de nosotros tengamos trabajo por el resto de la vida.

Desde la perspectiva operativa, no sé de qué manera puedo explicarles algunos de mis clientes por qué ciertas cosas no funcionan porque ya están lo suficientemente mal las cosas ahora cuando nos llaman y nos dicen que tienen un problema con

Outlook cuando en realidad no usan Outlook porque piensan que Outlook es el cliente. Firefox es el único browser que tienen.

Entonces, hay algunas cuestiones operativas interesantes que tendremos que enfrentar en los próximos meses cuando esto pase a producción en algunos ISPs, veremos nuevas cuestiones. Encontrarán maneras de usar tecnología, los registros TXT y DNS los usarán para propagar malwares. Yo hice una presentación y lo vi hace poco. Me preocupa mucho eso pero no sé por qué me tiene que preocupar tanto. Bueno, es un chiste. Pero creo que es algo que vamos a tener que seguir esto más de cerca.

A mí me preocupa mucho personalmente esta idea de entregar ese control, esa decisión. Veo mi propia red empresarial. ¿Dónde vamos a poner nuestras cosas, nuestro contenido protegido de malware y otro tipo de ataques? ¿Tenemos la tecnología para ello? Imagino que la respuesta es no. Ahora, ¿es esto fundamentalmente algo malo? La respuesta es no, pero deberá tener cierta evolución.

ALEJANDRA REYNOSO: Gracias, Michele. Ahora preguntas para los panelistas, tengo el número seis. El número cinco después. Sí, por favor, el número seis.

MILTON MUELLER: La palabra concentración surge en muchas discusiones. Alguien que hace análisis económico no necesariamente considera que concentración y consolidación son palabras malas. Yo entiendo que estos servicios no son perjudiciales. ¿Hay alguna preocupación de que esta concentración lleve a un aumento de los precios de los servicios de DNS? ¿Podría especificar más exactamente cuál es la preocupación y cómo el mercado general va a ser afectado?

VITTORIO BERTOLA: Yo no creo que sea una gran preocupación porque los ISP actualmente brindan acceso de servicio. No es una concentración de información ni control la cuestión. Por ejemplo, al encriptar el contenido, se da privacidad, pero si en definitiva terminamos con que todos usen el mismo resolutor, ese resolutor va a ver el contenido del 60% del mundo. O sea, ahí se pierde mucho la privacidad también, ese es el peligro.

MICHELE NEYLON: Creo, Milton, no tiene que ver con el precio, sí con el funcionamiento de la internet porque es distribuida, es una red de redes. Cada ISP puede configurar sus propios resolutores, cada red… Incluso nosotros podemos tener dentro de cada ISP nuestros propios resolutores, entonces si empezamos a

concentrar, se pierde la estabilidad y la resiliencia que puede desaparecer. Y también esta loca cantidad de datos que hay en el tráfico por el DNS, no sólo lo que está, sino lo que no está. Lo que la gente intenta ver que no existe y eso vale muchísimo dinero.

ALEJANDRA REYNOSO: Muchas gracias. El cinco.

ORADOR NO IDENTIFICADO: Hay una confusión. Cuando se habla del DNS a nivel del navegador, eso es a nivel de usuario. ¿Quién aplica la política entonces? ¿Cómo aportamos claridad a nivel de política? Esa es la pregunta. Gracias.

TIM APRIL: ¿Quién tiene el mandato de encontrar la política que se implementa en el browser, en el navegador? ¿Eso es lo que usted está preguntando? Bueno, eso depende del fabricante del navegador. Son ellos los que dan el feedback y son ellos los que eligen la implementación. No hay ningún mecanismo de política para obligarlos a hacer nada, pueden hacer lo que quieren.

ALEJANDRA REYNOSO: Gracias. Número tres.

EDUARDO DÍAZ: Gracias, soy Eduardo Díaz de NARALO. Es posible que si yo me convierto en una gran empresa con un gran resolutor, ¿puedo empezar a vender o a ofrecer un dominio de alto nivel sin ir a la ICANN? Y los otros resolutores también me pueden contactar porque yo soy un grupo final, ¿no? Eso debería poder ocurrir, ¿es correcto?

TIM APRIL: Sí, es técnicamente posible. No hay nada que prohíba eso.

DANNY MCPHERSON: Yo no creo que DoH o DoT cambie en nada eso.

TIM APRIL: Es muy parecido a lo que sucedió con el .onion

ALEJANDRA REYNOSO: Número cuatro.

FRED BAKER: A mí me preocupa el ruteo de internet. Ustedes seguramente están familiarizados con el caso, pero voy a tratar de evitar mencionar el nombre. El tema puede ser un tema de empresa

también, imponer modelos de seguridad de información que se hace en parte denegando acceso a este tipo de nombres de un modo u otro.

Ahora, la entidad en la que estoy pensando, la gente que está en ese lugar, desea empezar a utilizar el resolutor de Google y se circunvaló esas características a través de la empresa que atacó al resolutor de Google. En el punto en el que hay una solución de seguridad que se convierte en tomar un ruteador, a mí me interesaría saber cuáles son los comentarios.

DANNY MCPHERSON: Yo diría que el sistema de ruteo es una forma de confianza y uno elige creer lo que a uno le dice y lo propaga o no, no hay ninguna autoridad central hoy. Hay algunas técnicas donde cualquier que opera a cualquier infraestructura técnica tiene que utilizar esa técnica para asegurar el sistema de ruteo, pero sé que el sistema de ruteo es una de las inquietudes de seguridad más preocupantes.

TIM APRIL: Y también está el caso de considerar utilizar DNSSEC y los resolutores [Ivein]. Cuando el resolutor está haciendo un pedido trata de contactar al servidor y valida el certificado a través del DNS y utiliza DNSSEC para validarlo. Esto al servidor al que le está

hablando donde uno si está en un área que tiene acceso a la confianza, uno puede confiar entonces en el chequeo de un certificado a través del chequeo de la confianza.

ALEJANDRA REYNOSO: Gracias. Número seis.

MARK SVANCAREK: Respecto de la pregunta a la audiencia. Una inquietud que surge mucho es la concentración de los proveedores de DNS. ¿Por qué eso no es la pregunta en lugar de que sean estos protocolos? Si el navegador más popular va a ir a quad 8 y ya hay una concentración importante más allá de esos protocolos porque ese no es el problema que más nos preocupe y simplemente eso acelera la tendencia. Yo creo que eso debería ser uno de los puntos además de estas preguntas de protocolo.

TIM APRIL: Warren estaba diciendo que Chrome no va a seleccionar quad 8 por defecto, es decir, que solamente—

ALEJANDRA REYNOSO: Por favor utilice el micrófono.

TIM APRIL: Warren me puede corregir, pero la forma en la que Chrome planee implementar los que por defecto, si el sistema del resolutor acepta DoH va a tener una forma de resolución y el sistema puede seleccionar utilizar DoH con cualquier resolutor. Es decir, que podría seleccionar quad 8 incluso si hay una opción pre-configurada en el menú desplegable.

VITTORIO BERTOLA: Quisiera agregar algo un poco más general. Muchos de los temas en términos de seguridad que hemos estado hablando ya existen hoy cuando un usuario ingresa, por ejemplo, en servidores de quad A. El punto es que esto está siendo el defecto, por eso van llegando a los distintos resolutores. Yo estoy de acuerdo en que cualquier tipo de concentración es ya una preocupación.

Me alegra que Google diga que ellos no van a adoptar este modelo de implementación, pero por supuesto, hay que ver lo que pasa dentro de 5 o 10 años.

ALEJANDRA REYNOSO: Número cinco.

ROBERTO GAETANO: Gracias. Soy Roberto Gaetano usuario de internet. Soy lo suficientemente grande como para haber visto los tiempos en los

que el software de red, y varias soluciones propietarias que hacían un poco de todo en distintas partes, y luego tuvimos una arquitectura de siete capas con una capa de transporte, otra capa física, etcétera y el resultado fue la posibilidad de tener software abierto, de tener soluciones que para cada capa podían competir con otras.

Con este tipo de abordaje del DoH y el DoT, ¿no estamos retornando a las soluciones propietarias que limitan la posibilidad de tener soluciones que compiten y devolver a lo que ocurría en los años 60 que se llama inadecuadamente, especialmente para mí, el código espagueti?

DANNY MCPHERSON: Creo que es un punto justo este. Todavía se usa el modelo TCP IP o resolución over the pop en lugar de utilizar un resolutor stub en el sistema local. Si vemos difusión en el camino de resolución en el sistema local y todo eso se circunvala, puede haber implicancias en el usuario, en el operador de red, en la infraestructura y en todas las distintas partes que pueden beneficiarse o que pueden perder también de alguna manera.

Yo entiendo su punto por un lado y, por el otro, no creo que se esté saliendo de ahí. Si usted tiene solamente aplicaciones de usuario finales y se puede decir directamente a la infraestructura

qué es lo que quiere, se puede ver los dos lugares de la transacción o las dos caras de la transacción. Se puede incluir a los operadores de red y actualizar sus resolutores para que haya mejores capacidades y otras veces el usuario puede tener una resolución y utilizar algo que puede resultar problemático.

PETER KOCH: Roberto, tanto usted como el orador anterior, no dijeron que está en silos. Esta es una tendencia que no tiene inmediata ente que ver con la estandarización de estos dos protocolos y, seguramente, son muy inocentes, peor están siguiendo una tendencia general. La mayoría de ustedes tienen aplicaciones en sus teléfonos inteligentes y ha habido largas discusiones sobre lo que eso significa para la estandarización y, por supuesto, también para la infraestructura central del usuario.

Cuando yo utilizo aplicaciones, ¿cuál es el nivel de HTTP que yo puedo hacer por mí mismo? Eso es parte del panorama general. No es lo único, pero es otra tendencia y se trata de la infraestructura de la cual se ocupa ICANN. Y por eso hay importantes razones por presentar esto aquí ante esta audiencia.

ALEJANDRA REYNOSO: Gracias. Número tres.

JÖRG SCHWEIGER: Soy de Denik. Entiendo que la conclusión es que ya sea que DoH es malo o extremadamente malo depende del modelo de implementación, pero me pregunto si esto es cierto. Si solamente el usuario tiene elección, sería beneficioso utilizar DoH. Pero tomando en consideración que el usuario puede descargar una aplicación, luego el camino de resolución va a estar enterrado muy profundamente en la aplicación. Es decir, que actualmente no hay ningún tipo de elección y el App Store va a pertenecer a un jugador de los más grandes y, en ese caso, no hay ningún tipo de elección. ¿Tiene que ver entonces esto con el modelo de implementación?

VITTORIO BERTOLA: Esta ha sido una discusión también en el IETF. Hasta qué punto este es un tema de protocolo y hasta qué punto es la forma en la que la gente lo usa. Creo que lo importante es que entendemos si puede haber una discusión y cuáles son las partes interesadas porque si la aplicación le puede dejar al usuario elegir, o incluso si puede configurar lo que está por defecto y hay una regla. En ese caso, la mayoría de los problemas deberían desaparecer.

El punto es, ¿cómo podemos tener esa conversación? Hay muy poca gente aquí de los fabricantes de navegadores, entonces,

¿cómo podemos incluir a esta gente en las discusiones sobre las políticas?

ALEJANDRA REYNOSO: Tenemos dos preguntas remotas. Por favor.

ARIEL LIANG: La primera pregunta remota es de Christopher Wilkinson. La concentración ha sido un tema global desde hace más de 20 años, los operadores, los servidores de raíz, los ISP, etcétera. ¿Por qué ahora deberían ir en una dirección opuesta? ¿Estos resolutores dónde van a estar ubicados? ¿Cuál va a ser el costo y la seguridad?

VITTORIO BERTOLA: Un punto que quisiera mencionar es que las plataformas de resolutor pueden ser distribuidas en cada país, pero si la empresa sigue teniendo o estando en una jurisdicción en particular, en ese caso yo estoy de acuerdo con lo que ha dicho Christopher.

DANNY MCPHERSON: El sistema de servidores de raíz podría ser quizás la forma de resolución de servicios de internet más distribuida del mundo. Yo creo, hemos hecho un trabajo de híper gigantes hace 20 años

donde las entidades de internet representaban el 85% del tráfico y, ciertamente, si esas entidades operan, los ISP y otros no pueden proteger la confidencialidad de los datos confidenciales. En ese caso las receptividades van a ver más tráfico y ahí podemos ver temas jurisdiccionales y otros.

El capitalismo y la economía nos van a poder ayudar. Esta es una tecnología Naciente. Creo que todavía tenemos que esperar un poco.

ALEJANDRA REYNOSO: Segunda pregunta.

ARIEL LIANG: La segunda pregunta es de Mike Bagley. ¿DoH permite bypasear mejor el DNS y también detiene los adblockers? ¿Esto no sería aumentar los riesgos de seguridad?

MICHELE NEYLON: La respuesta corta es que sí.

DANNY MCPHERSON: Yo lo que dije en mis diapositivas es que la resolución del DNS ocurre con el mismo protocolo y con el mismo destino que lo que ocurre en la capa de aplicación y donde ocurre el tráfico web.

Cualquiera que quiere manipular eso, va a tener que trabajar un poco más para ver qué es lo que quiere manipular. Y francamente, este es uno de los temas aquí, hay personas que manipulan las respuestas de DNS y si se trata de un proveedor de navegadores o un operador, se puede seguir manipulando las respuestas y, en ese caso, se puede impactar en la parte económica. Es decir, que va a haber ganadores y perdedores allí también.

A mí me parece que los sistemas de seguridad van a tener que estar a la altura e incluso se pueden bloquear estos protocolos en un Enterprise que es lo que muchas empresas van a hacer. Es decir, van a colocar un proxy y no van a permitir que ocurran las resoluciones. Incluso desde la perspectiva de la soberanía.

ALEJANDRA REYNOSO: Número cuatro.

KAVOUSS ARASTEH: Muchas gracias. Quiero hacer algunos comentarios en lugar de hacer preguntas. Usted preguntó cuántos de nosotros entendemos DNS. Yo no puedo responder y no puedo hablar aquí por nadie. Esa es la declaración que usted hizo. Usted también dijo si estamos preocupados por la seguridad, la respuesta es sí. ¿Estamos preocupados por la privacidad? Sí. ¿Estamos

preocupados por la tecnología? Sí, pero para algunos de nosotros, no muchos de nosotros, estos son los temas nuevos. Tenemos que digerirlos, tenemos que poder entenderlos.

Antes de responder cualquiera de estas preguntas, tenemos que tener tiempo para ver cómo funciona y si es que se responde al tema de las seguridad y de la privacidad.

Es una pregunta o un tema que debemos ir siguiendo y es difícil poder responder a cualquiera de estas preguntas. Incluso la pregunta dos que está directamente vinculada con la misión de la ICANN. Quizás tengamos que agregar más preguntas. Muchas gracias.

MICHELE NEYLON: Gracias, Kavouss. Por primera vez estamos de acuerdo, eso no ocurre mucho. Esto es algo que es muy nuevo y muchos de nosotros hemos hecho referencia a que es nuevo, es una tecnología naciente. Muchos de nosotros hemos tratado de alentar a la gente en distintas partes del ecosistema a empezar a formular esas preguntas, a hacer la pregunta simple, también la compleja y la verdaderamente difícil. A nivel teórico y también hablar con las empresas que ya están implementando esas tecnologías. Y ellos van a decir, “bueno, está bien, lo que nosotros estamos haciendo es para el bien común”. Pero una vez que uno

los pone sobre el microscopio, no sabe si eso va a ser así siempre. Es algo que puede empezar como algo inocente y que se puede convertir en otra cosa o quizás siga siendo inocente.

Es algo que todos tenemos que analizar y quizás contactarse con alguno de ustedes aquí en la sala o fuera de la sala y continuar esta conversación porque esto es algo que ha sido discutido en IETF y en los círculos técnicos. Creo que hace tres o cuatro años quizás más, empezó con la pregunta del cómo podemos hacer el DNS más privado y después cada vez más seguido parecido a esa pregunta.

Pero para las personas que no están en el IETF y los geeks, ahora esto se está convirtiendo en una realidad y ya es momento de que empecemos a tener esas conversaciones.

ALEJANDRA REYNOSO: Gracias. Pregunta cinco.

ANDY BATES: Gracias. Soy Andy Bates de la Cyber Alianza Global. Me parece que este es un muy buen debate sobre la consolidación. La pregunta a los panelistas es: Nosotros no queremos continuar con el DNS normal, ¿deberíamos nosotros de utilizar alguna de estas

soluciones? Estamos hablando de proteger al usuario sobre el ciberdelito. Quisiera escuchar su opinión.

VITTORIO BERTOLA: La encriptación es algo positivo, es algo que debemos hacer. Los operadores les decimos que implementen DoH, pero algunos… Estas cuestiones crean problemas de seguridad que son cada vez más grandes y en ese caso no podemos hacer un avance. Lo positivo de aquí es entender lo que está ocurriendo, compartir la política para poder así maximizar lo positivo y lo negativo.

ALEJANDRA REYNOSO: Muchas gracias. La número tres.

WOLFGANG KLEINWAECHTER: Esta es la sala del GAC. En las diapositivas identifiqué algunas dificultades para el marco de los organismos de aplicación de la ley. ¿Ustedes ven algún tipo de impacto para ellos aquí?

MICHELE NEYLON: Hola, Wolfgang. Nosotros no estamos a cargo de esto. A ver, somos personas a las que nos pidieron hablar de esto por distintas razones, pero esa pregunta no nos la tiene que hacer a

nosotros. Vittorio, por supuesto, me va a contradecir, pero para eso vino al panel. Peter me va a contradecir.

PETER KOCH: Por primera vez en la vida, Michele. Excelente pregunta, sí. Hay algunos aspectos de este debate sobre el bloqueo. Hay gobiernos que creen en el bloqueo del DNS, que esto prevendría el alcance a ciertos contenidos por parte del consumidor, pero es muy fácil de eludir esto.

Por otra parte, la resolución de los nombres de dominio cuando se usa para prevenir accesos accidentales a contenidos o lo que fuere, estamos hablando de malware, phishing, etcétera, contactar botnets para que tomen el control de nuestros sistemas, bueno eso podría funcionar, pero nada dice que los proveedores de resolución, algunos ya hoy ofrecen ciertos servicios, protección de DNS, no sé si está ya registrada la marca pero hay firewalls. Lo agregan como servicio adicional.

Y volviendo a lo que preguntaba Milton, sí, algunos cobran un monto. Algunos cobran en términos de datos, pero esa es otra cuestión. Pero algunos cobran dinero por darnos listas negras de sitios de phishing y malware y no hay motivo por el cual esto no sea desplegado por algunos proveedores con los cuales hemos venido hablando, así que no todas las historias de regulación

pueden ser eludidas fácilmente ni dadas por sentado. Hay dificultades, hay detalles y si usted es un defensor del bloqueo del DNS, va a creer, va a defender el bloqueo del DNS sobre DoH o DoT.

VITTORIO BERTOLA: Yo no creo, no defiendo el bloqueo. La decisión importante es que este bloqueo por sí o por no se tome democráticamente en la comunidad y que no la tomen esa decisión las compañías de browsers. Creo que es en ese sentido este debate.

Algunos de los proponentes del DoH hemos tenido entrevistas y hablan del control de censura, incluso en países democráticos. Esto es algo que para los ciudadanos europeos hace mucho ruido. Los gobiernos, no sé si hay algunos que se están ocupando, pero aquí son más que bienvenidos.

ALEJANDRA REYNOSO: Pasamos al número cuatro y cerramos la lista con un participante remoto.

SÉBASTIEN BACHOLLET: Hablaré en francés ya que contamos con los servicios de interpretación, hay interpretes muy calificados en la sala.

Yo soy usuario individual de la internet y miembro de ALAC. Tengo una pregunta que me interesa, son dos preguntas. Primero, ¿cuál será la elección del usuario final cuando existe el riesgo de encontrarse en una situación como la de hace algunos años con los servidores que no podían ser accedidos? ¿Habrá otras cuestiones? Alguien puede elegir por el usuario cómo se va a dar la resolución.

Y mi segunda pregunta tiene que ver con el hecho de que nosotros estamos en la ICANN. ¿Cuáles son las consecuencias posibles respecto de los nombres, respecto de los servidores raíz y respecto de la manera en que todo esto va a ser manejado en el futuro? ¿Podemos imaginar que la ICANN dejará de existir? Porque estos resolutores servidores podrían decidir que el añadir en sus archivos nuevas extensiones, nuevos archivos o sacarlos. ¿Esto va a bloquear cosas, añadir cosas? Estas preguntas son importantes en mi opinión.

Y estoy de acuerdo con lo que dijo antes. Es importante que sigamos trabajando en estas cuestiones. Es muy mal que la estandarización se haga incluso antes de poder discutir estos temas sin todas las partes interesadas. Muchas gracias.

MICHELE NEYLON: Gracias por su pregunta, Sébastien. Muchas de esas preguntas ya las tratamos en la sesión anterior. Sí, existe el potencial de que algunos proveedores decidan qué hacer y, como decía antes, es posible oponerse al bloqueo, pero es un riesgo. Los protocolos y los estándares son cosas que se desarrollan por parte de gente en organismos de estandarización como el IETF donde se discute y se pueden seguir esos debates. Son abiertos, por supuesto la barrera es técnica. No es para cualquiera. Son estándares que impactan sobre nuestra vida cotidiana, pero la mayoría de nosotros no tenemos la menor idea de lo que están hablando porque no es nuestro expertiz.

El poder tener estas discusiones es muy importante, tal como la discusión de ahora. No sé si alguien quiere agregar algo más.

TIM APRIL: Voy a agregar lo siguiente: Las tecnologías DoH y DoT no son inherentemente los culpables per se, es más la implementación. DoH, DoT son estándares propuestos del IETF, pero podrían haberlo implementado directamente las empresas de navegadores web.

¿Por qué es un tema tan candente ahora? Porque hay una propuesta de una norma, o sea, añadir este mecanismo de privacidad a la primera milla de las solicitudes al DNS lo que

generó este interés. Si se ponen bloqueos en este despliegue, me imagino que la gente inteligente que tiene el IETF va a encontrar otras maneras de hacerlo.

ALEJANDRA REYNOSO: Pido disculpas por la interrupción, pero tenemos que tomar la última pregunta remota y nos quedamos sin tiempo. Disculpa por la interrupción, podemos seguir la conversación en los pasillos después.

ARIEL LIANG: En realidad es un comentario de Paul Hoffman. DoH y DoT son protocolos nuevos que las aplicaciones y los sistemas operativos han venido haciendo de manera similar desde hace más de 20 años.

VITTORIO BARTOLA: Es uno de los autores él, en realidad, de la norma, pero está bien.

ALEJANDRA REYNOSO: Ahora voy a cerrar con esta sesión y le voy a pedir a cada uno de ustedes muy rápidamente que nos diga algo que la gente aquí pueda llevarse como mensaje esencial. ¿Les parece? Gracias.

TIM APRIL: Como decía, DoH y DoT son las dos normas propuestas desde el IETF que no añade capacidades técnicas al sistema de nombres que no estuvieran ya disponibles a través de los métodos estándar. La gran preocupación, por lo menos en mi opinión, es que lo que estamos discutiendo terminará en un resultado que dependerá de los despliegues, de las implementaciones y los detalles de los protocolos a futuro.

VITTORIO BERTOLA: Mi mensaje simplemente es seguir trabajando en comprender este tema. Aun cuando esta sea la primera vez que están frente a este tema, hay mucha gente dispuesta a ayudar y materiales en la internet. Pueden participar desde las distintas partes interesadas, pueden participar a través de organismos de política aun cuando los temas ahí quizás sean más técnicos y políticos.

PETER KOCH: Quiero decir que las normas que salen del IETF son cruciales para los desarrollos que veremos, pero no son la causa raíz y debemos hablar de la causa raíz y tener este gran panorama, esta gran concepción de lo que esto significa para la ICANN y para la gobernanza del espacio de nombres.

DANNY MCPHERSON: Sí, desde la perspectiva operativa hay costos adicionales, pero también un efecto en términos de privacidad y seguridad. Cuando entendamos cómo se desplegará, sabremos las implicancias. El SSAC está comenzando recién ahora a considerar esto y sin duda agradeceremos sus opiniones. Es un blanco móvil, son normas que están todavía en desarrollo en el IETF. Hay que entender entonces cuáles son las implicancias para la ICANN y la gente de política.

Esperamos que la gente que hace política en la ICANN con el asesoramiento del SSAC puedan hacer una mejor labor. Gracias.

MICHELE NEYLON: Alejandra, usted hizo algo muy peligroso que es darme la última palabra.

Creo que los comentarios de las preguntas aquí en la sala y remotas han sido muy interesantes. Yo en lo personal tengo ciertas, tenía ciertos sentimientos respecto a estas tecnologías antes de venir aquí y creo que por las preguntas y comentarios que nos hicieron, mi propia visión sigue en evolución.

Esto quizás signifique que vamos por el camino correcto cuando decidimos hacer esta conversación. Entonces mi mensaje para ustedes es, fíjense en la diapositiva en este momento en pantalla. Hay un par de puntos que indican dónde pueden encontrar más

información. La próxima reunión de la IETF creo que es dnsprivacy.org ese sitio que tiene mucha información sobre las tecnologías subyacentes, muchas publicaciones en distintos blogs, en distintas compañías y de otros grupos. CENTR creo que hizo un paper hace poco. Si tienen tiempo, lean un poco más y hagan preguntas.

ALEJANDRA REYNOSO: Muchas gracias. Y se cierra la sesión. Un aplauso a los panelistas.

[FIN DE LA TRANSCRIPCIÓN]