GISELLA GRUBER: Buenos días, buenas tardes y buenas noches a todos. Bienvenidos al programa de seminarios web de creación de capacidades, hoy vamos a hablar de DoH, DoT, beneficios, inconvenientes en el camino a futuro, el 07 de septiembre del 2020 a las 21:00 UTC. Durante 60 minutos Holly Raiche será la presentadora y Joanna Kulesza hará una breve introducción después de mí.

No registraremos asistencia, pero los participantes quedarán registrados en la página. Tenemos interpretación al español y al francés, por favor digan su nombre cada vez que tomen la palabra para que nuestros intérpretes le identifiquen en los canales respectivos de idiomas y también para la transcripción. También tenemos transcripción en tiempo real, el vínculo está en la página Wiki y también está en el chat.

Es muy importante que se hable a una velocidad razonable, con claridad para permitir una interpretación precisa, todas las líneas estarán en silencio durante la presentación y podrán hacerse preguntas al final. Si están en la sala de Zoom, levanten la mano y la moderadora los incorporará a la lista o pueden escribir una pregunta en el chat, en el formato que acabo de exhibir en el chat.

Haremos un seguimiento de todas las preguntas que serán contestadas durante la sesión de preguntas y respuestas o bien, pueden levantar la mano y formularlas por audio para ser más interactivos, si están en el puente telefónico, por favor soliciten que se les agregue a la lista de preguntas. Sin más, le paso la palabra a Joanna Kulesza, copresidente del grupo de trabajo de creación de capacidades. Muchas gracias por su atención. Adelante, Joanna.

JOANNA KULESZA: Muchas gracias, Gisella. Bienvenidos a otro seminario web sobre un aspecto técnico del DNS y la gobernanza de internet, trataremos un acrónimo muy interesante para la comunidad At-Large y más allá, DoH y DoT y tenemos a una presentadora muy apropiada, Holly Raiche. Seguramente ustedes la conocen, quienes están en At-Large tiene una vasta experiencia en la gobernanza de internet, ha sido conferenciante y ha hecho muchas presentaciones en Australia y en otros países.

En nuestra agenda encontrarán el vínculo compartido por Gisella. Para tratar de ser lo más breve posible, la idea es hablar solo 5 minutos según la agenda, pero prefiero dejarle más tiempo a Holly para su presentación. Tenemos también 20 minutos para la sesión de preguntas y respuestas, como dijo Gisella, nos gusta la interactividad, así que tienen tanto la posibilidad de escribir como de hablar, levanten la mano y se abrirá el micrófono para la pregunta.

Nos gustaría reunir todas las preguntas después de la presentación, todos los comentarios, todo lo que tengan en mente pueden compartirlo libremente a través del chat indicando que tienen una pregunta, tal como en el formato que mostró Gisella.

También les vamos a solicitar un feedback breve, es uno de los abordajes que tenemos para nuestros webinars para mejorar las necesidades de la comunidad de la ICANN, así que les vamos a preguntar qué han pensado, si tienen alguna reflexión sobre el evento, áreas de mejoras o sugerencias.

Aquí le paso la palabra a Holly y muchas gracias por aceptar nuestra invitación para tratar estos acrónimos tan ambiguos, sabemos que nos gustan mucho los acrónimos. Adelante, Holly, por favor cuéntanos qué significan estos acrónimos, si es algo bueno, si es algo malo para los usuarios finales y todo lo que podemos conocer en relación con las políticas.

HOLLY RAICHE: Muchas gracias, Joanna. Y debo decir que hay mucho para decir, pero ante todo quiero adelantarme y decirles que no he preparado preguntas porque no es un tema que se preste demasiado a ello, sin embargo, aclaro que es un tema que arranca como algo muy técnico y yo en lo personal no tengo los conocimientos técnicos para formular las preguntas.

Geoff Huston, que está en el grupo, es una de las personas muy capacitadas que tiene un blog. Geoff es también miembro de un grupo especializado en Australia. Es uno de esos temas donde la tecnología misma plantea preguntas, tanto para los usuarios finales como para quienes estamos en el aspecto no técnico. Espero que esto no lleve mucho más de media hora.

Empecemos por hablar un poquito de qué es la terminología, cómo funcionan, qué significan, cuáles son los propósitos para introducir estas tecnologías, sus ventajas, sus desventajas y cuál es el camino a futuro. Quienes han asistido a las reuniones de la ICANN recordarán que hubo dos sesiones sobre este tema, la primera fue una sesión más técnica en Kobe en la última reunión presencial que tuvimos y la segunda fue en marzo, en una de nuestras reuniones virtuales.

Así que imagino que muchos de ustedes, este tema lo encontrarán familiar, aunque quizás no todos, al final le voy a pedir a Geoff que nos comparta algunas preguntas también. Segunda diapositiva por favor.

Esta terminología básica, asumo que la mayoría de ustedes conocen, comprenden cómo funciona el internet, pero por las dudas aclaremos. ¿Qué es un mensaje del DNS o cómo se usa en este contexto? E hice un diagrama para describir el proceso del que hablamos, que es crítico el concepto para entender la cuestión.

En esencia es un protocolo de consultas y respuestas, cuyo propósito es convertir lo que uno escribe en el navegador, convertir lo que uno escribe en una serie de números que es la dirección IP que saldrá de la computadora o del teléfono o del dispositivo a otro, del mío al de ustedes. DoT que es uno de los términos que vamos a tratar hoy, es nombres de dominio o DNS sobre la seguridad de la capa de transporte o TLS.

TLS es el protocolo seguro cuyo propósito es otorgar privacidad e integridad de los datos. La capa TLS es esa capa donde viajan los paquetes de la dirección IP de una computadora a otra o de un dispositivo a otro. DoH, seguramente ustedes esto ya lo saben, cuando ven HTTPS, la S representa seguridad, o sea es el protocolo de transferencia seguro, es la versión segura del protocolo primario que se usaba para enviar datos entre un navegador web y un sitio web.

Ambos términos notarán que se refieren al concepto de privacidad y seguridad. Seguridad, en el sentido de que los datos que viajan de un lado al otro son seguros. Middlebox es un término que usó Paul Hoffman en sus presentaciones, es un termino genérico, es un dispositivo que se

encuentra entre el cliente y el servidor que analiza y quizás modifica el tráfico, puede ser un Firewall o puede ser la manera en que se introduce los filtros, algo que quizás analiza el contenido.

Es aquello que está en el medio, cuando los paquetes preguntan por primera vez a dónde ir y cuando los paquetes inician su viaje, eso en un momento lo van a comprender. La siguiente diapositiva por favor.

Espero que puedan ver el diagrama de la izquierda. Aquí estamos explicando de qué se trata, en el diagrama, empezando desde el ángulo superior izquierdo, escribo una dirección, supongamos que escribo ICANN.Org, esa dirección va al resolutor que se encuentran en los números que envían el paquete hacia su destino, a esta dirección.

Entonces los paquetes parten del resolutor y llegan aquí que es el servidor raíz, que antes se llamaba IANA y ahora se llama PTI y dice: "¿A dónde tengo que ir? ¿Cuál es la dirección que me va a enviar en la ruta correcta? IANA o PTI le dirá: "Usted tiene que ir a PIR". Una vez que tiene esa información, ya sabe que tiene que ir a ICANN y luego sabe que hacia atrás en este viaje tiene que ir a At-Large.

O sea, recibe una respuesta con una serie de números, la dirección IP que vuelve a mí y dice: "Ok, ahora tenemos el mapa, la hoja de ruta hacia donde tengo que ir, vamos". ¿Por qué destinamos todo este tiempo para explicar estos viajes o estas rutas en rojo? Están sin encriptar, la cuestión es esta área que no tiene encriptación la que puede generar preocupación.

Cuando se envían los paquetes en ese viaje, estos paquetes pueden ser encriptados, pero en una dirección típica no lo están y eso genera

muchas posibilidades, abre la posibilidad de filtración, protección contra abuso de menores, etc. La siguiente por favor, la siguiente por favor.

Recientemente ha habido menos consciencia de que la búsqueda lleva a esto, el proceso de búsqueda queda sin estar encriptado, incluso si utilizamos DNSSEC, TLS y otras cuestiones de seguridad, sigue esta parte roja que está no encriptada, por lo tanto, el uso indebido del DNS queda abierto y esto cada vez es una inquietud más importante, puede haber Spoofing, etc.

Ciertamente está también el tema de la privacidad y después de lo que sucedió con Edward Snowden, todo el mundo está mucho más consciente de cuánto es el material no encriptado, se busca, se utiliza y se utiliza indebidamente incluso. Y yo agregaría también el consentimiento, si miramos cuándo será o no será libremente el consentimiento, aquí es donde todos estos datos se empiezan a recolectar.

El otro asunto es que en ese espacio rojo es donde ocurren los controles, sufrimos el uso indebido del DNS, la pérdida de la privacidad, pero ganamos en control. Siguiente diapositiva, por favor.

Para que quede más claro, el único cambio es agregar algún tipo de encriptación de seguridad en ese procedimiento de búsqueda, ningún cambio a las consultas y a las respuestas, ni tampoco ningún cambio que no esté encriptado es de un protocolo DoH o DoT en sí.

Es decir, que simplemente hacer una búsqueda o, mejor dicho, encriptar de alguna manera lo que no estaba encriptado hasta ahora. Siguiente diapositiva.

En el año 2016 empezó a haber una toma de consciencia sobre lo bueno y lo malo que ocurre por la naturaleza de lo que no está encriptado, en el proceso de búsqueda en el DNS.

Lo que sucede con DoT es que se agrega encriptación en el TLS, es decir, que tenemos el Sistema de Nombres de Dominio corriendo en TLS, entre la computadora del usuario final y el resolutor recursivo encontramos el primer punto que está en mi diagrama, no después. Es decir, que estamos hablando un poco más de la capa de transporte de mensajes en DNS cuando tomamos el modelo de Paul.

Esta es una ilustración de cómo es un proceso de búsqueda en el DNS o en una red hogareña, esto no está encriptado, va del navegador a la computadora y esto sí está encriptado. Este es todo el proceso del resolutor recursivo al que yo estaba apuntando y esto no está encriptado, lo que esto hace es que deja de funcionar o quiebra digamos, la conexión entre quiénes son ustedes y a dónde van. Siguiente diapositiva por favor.

Para una red empresaria, seguimos todavía en DoT, aquí es donde se coloca la encriptación, de nuevo, esto no está encriptado y esto tampoco, pero la conexión entre quiénes son ustedes y a dónde van está interrumpida también aquí. Siguiente diapositiva.

DoH es un poco más sofisticado; es una versión de capa de cómo se agrega privacidad o cómo se protege, es decir, que el proceso de búsqueda real. De nuevo, esta es una presentación general, los mensajes van a estar incluidos en HTTP y van a ser transportados corriendo en TLS. Es decir, que va a haber más protección o encriptación.

Se permite que se tomen las respuestas del DNS antes de que se soliciten y aquí es entonces donde nos preocupa la replicación de tráfico de DNS. También hay alguien más en el mundo de ICANN que hizo su propio paper de DNS que desarrolló en el sitio web, el documento SSAC109, se publicó en el mes de marzo cuando ocurre la segunda sesión sobre DoH, DoT y se habla de transacciones en el DNS, es decir, que TLS transporta los paquetes y dado que la transacción de DNS está oculta en el HTTPS, simplemente avanza.

Incluso a nivel de gobierno hubo una investigación del congreso de Estados Unidos y ellos no hablan de DoT, solamente hablan de DoH y en el… Solamente utilizan navegadores, no utilizan a terceros y aquí es donde vemos que hay un tema con la falta de privacidad, la recolección de datos y los problemas con la seguridad.

Ven acá que la flecha es mucho más grande en este diagrama, aquí DNS está en la capa de transporte y va hasta acá. Aquí vemos que hay más seguridad y, de hecho, puede atravesar un proceso normal en el camino hacia el resolutor que va a elegir el navegador. Siguiente diapositiva.

DoT puede ser identificado y bloqueado por un intermediario, como recordarán, DoH es el que pasa, DoH no es distinguible en el tráfico HTTP, por lo tanto, es más difícil de bloquear.

Es más difícil saber qué es lo que está ocurriendo desde el punto de vista del ISP, no se le puede bloquear a veces porque puede bloquear otro tráfico, es decir, que por un lado es más seguro, pero plantea otros problemas también. Los gobiernos finalmente están empezando a estar interesados, y me gusta a mí mucho esta cita de La Baronesa Thornton

donde hubo una discusión en el Reino Unido, un debate respecto de qué es esto.

La Baronesa está preocupada por una pregunta un poco geek sobre el DoH. Lo que finalmente preocupa a los gobiernos es la falta de rendición de cuentas respecto de lo técnico. Ella está hablando aquí del IETS. En general, son empleados de grandes empresas de internet bueno, esto puede ser o puede no ser y ellos toman decisiones que tienen implicancias políticas y enormes consecuencias para todos nosotros y ella pregunta: ¿Cuál es la relación que ha tenido el gobierno británico con el IETS?

Y seguramente no sabe que hay mucha participación con ingenieros, pero aquí se destaca el hecho de que el gobierno está finalmente empezando a preguntar qué ocurre. La Cámara de los Lores, el informe del congreso de Estados Unidos, en todos esos lugares hay mucho debate sobre las implicancias de la tecnología. Para ambos; y estamos hablando aquí de las cuestiones a favor, ¿por qué lo haríamos? Bueno, por una cuestión de privacidad, ustedes como individuos hacia donde van es algo que habrá que definir, la conexión…

Es decir, ustedes se tienen que asegurar de que no hay una conexión entre ustedes y el resolutor, sino que todo el viaje del HTTP está protegido por DoH, es decir, dónde se recolectan todos esos datos es lo que a nosotros nos debe preocupar. Tenemos que preocuparnos si ambas tecnologías en la conexión entre ustedes y los datos, se ven interrumpidas o dejan funcionar.

Vamos a las cuestiones a favor. Si tenemos una búsqueda clásica, las consultas de DNS pueden ser interceptadas, el tráfico legítimo se ve

manipulado y como resultado, además de los temas de seguridad, puede haber una demora en los servicios y toda esa información sobre ustedes y hacia dónde van es recolectada.

También hay otras actividades maliciosas, categorías de uso indebido del DNS porque ahora estamos en DoH, estas cosas se pueden evitar ciertamente desde un punto de vista de seguridad, un ataque de DNS, Spoofing, etc.

Todo esto se puede prevenir, este es el proceso y estas son las cuestiones a favor. Y la razón por la cual no tengo una pregunta, es que no hay una respuesta fácil a qué es lo mejor, hay lados positivos y negativos, entonces lo que se evita con este proveedor de servicio es que pueda […] pueda abrir sitios web. No sé qué pasó ahora, ahora sí.

Se puede evitar que el email que típicamente envía malware, sea enviado, el ISP puede […] los servidores haciendo algunas activaciones y esta otra cuestión es algo que realmente llamó la atención del gobierno de Reino Unido, hay controles parentales, es decir, que los padres pueden evitar que los hijos vean ciertas cosas. Si estamos bloqueando el tráfico; esto ya no se va a poder hacer, hay muchos gobiernos que tienen régimen de filtrado y esto se puede pasar por alto.

Otra cosa que ocurrió es que muchas empresas que tienen información, van a verificar el tráfico que entra y sale del sistema y van a ver cuáles son los materiales que salen y quién los envía, cuáles son las medidas de seguridad que se pueden aplicar allí, sin embargo, se puede utilizar para evitar la comunicación con grupos disidentes, acceder a información y dar la información de a dónde uno va.

Eso es lo que sucede en todos los intercambios de información, con toda la información personal, lo que nosotros queremos es que no se divulgue por cuestiones de privacidad.

Se puede decir entonces que hay cuestiones a favor y en contra para el filtrado. Siguiente diapositiva, por favor.

Los beneficios, facilidad de configuración, tener un solo grupo de políticas del DNS que comprender y calles más grandes, esto lo señaló el SSAC que tiene que ver con el tráfico. Ahora se envía solo a los resolutores de confianza, uno sabe a dónde va el paquete y deja de ser un blanco, por así llamarlo, para los malos actores o para ataques de denegación de servicios, acciones maliciosas, etc.

Y como hay menos lugares donde el paquete puede ir, también existe la posibilidad de que el tráfico sea más lento, nuevamente, hay aspectos a favor y aspectos en contra. La siguiente.

¿En qué nos encontramos? Si se usa Firefox, ellos tienen el programa de resolutor recursivo de confianza. Y actualmente solo lo usan en CloudFlare y NextDNS, o sea el paquete va a uno de dos lugares, pasa por alto el proceso normal que sigue el DNS clásico y va hacia sus resolutores de confianza.

No sé hasta qué punto ha avanzado las pruebas con Google Chrome, Google tiene encriptación automática, Microsoft lo está empezando a estudiar. Esto ya ha dejado de ser un problema teórico, está aquí, está ahora, de hecho, yo estoy frente a mi computadora que usa Firefox sin Mozilla y bueno, me está pasando a mí. La siguiente.

De la publicación de Paul, a menos que los Middleboxes estén configurados de manera tal que se proteja la computadora, se permite cierta anonimidad, pero hay que permitir el control del Middlebox. Esto hay que considerarlo porque ahí es donde afecta la protección, ahí es donde está el control para entrar y ahí es donde se da cierta parte del filtrado.

Quizás podamos alejarnos un poco del DNS clásico, pero quizás exista una manera de preservar aparte de los datos, el Middlebox sigue, conoce los puntos de extremo del tráfico, el tráfico de confianza y entonces aplica políticas conocidas locales.

Entonces hay cierto espacio para preservar los aspectos positivos de la privacidad a través del filtrado. No conozco otras tecnologías que puedan ofrecer ambos beneficios. La siguiente diapositiva, por favor.

Estos son algunos vínculos de utilidad, en el sitio web de la ICANN pueden encontrar que en las dos reuniones donde esto se discutió, con Paul Hoffman y otros fueron el 12 de marzo de 2019 y un año después en la primera reunión en línea, están disponibles en los documentos, también en la oficina del director de tecnología y el documento del SSAC.

Hay un informe de cuestión del consejo de registros europeos de nivel nacional del servicio de investigación del congreso de Estados Unidos, también hay otro documento, hay mucha información, lo mejor es comenzar entonces por el sitio web con el documento de Paul y el paper del SSAC. Bueno, eso es todo de mi parte, gracias.

Nos quedan 20 minutos para preguntas y mi primera pregunta es, ¿qué pasé por alto? Quizás podamos empezar por el chat, Geoff…

GEOFF HUSTON: Muchas gracias, Holly. Muy clara su explicación. Si me permite, podría contribuir con algunos detalles. Antes me presento, yo soy Geoff Huston.

Hay una diferencia crítica entre DoH y DoT, y tiene que ver con el lugar de control, DNS solía ser aprovisionada por el proveedor de servicios de internet a través del sistema operativo, más allá de la aplicación que se corriera todas las consultas seguían la pila del protocolo, salían por el sistema operativo y eran enviadas al proveedor de servicios de internet para resolución.

DoT o DNS/TLS no cambia esta estructura, DoT es simplemente atípicamente como un protocolo de transporte por el sistema operativo y la idea por la cual las aplicaciones no se preocupan por la DNS sigue igual, entonces de alguna manera DoT es la infraestructura que conocemos. ¿Por qué generó tanta reacción DoH?

Porque DoH típicamente se implementa sobre la aplicación, entonces puedo tener ambos, Mozilla y Firefox y un servicio de correo electrónico o cualquiera otra aplicación. Y esa aplicación puede optar por hacer una consulta del DNS utilizando sus propios resolutores preferidos, sin hacer referencia a ninguna otra aplicación en el dispositivo.

Entonces ahora las queries van a todas partes o a cualquier parte y la solución propuesta por Paul Hoffman de darle a los Middleboxes una intervención entre la seguridad de donde quiero que vaya y donde va es

casi simplemente una buena práctica de seguridad. Los Middleboxes nunca comparten las claves secretas con el vecino.

Ese marco de solución que se propone, Holly, es efectiva, pero la cuestión concreta que está pasando por la cual se considera un problema, es que ahora el DNS ya no corre por canales que conocemos, la aplicación tiene la posibilidad de pasar por alto o enviar las queries a donde quiere sin hacer referencia del usuario final, ni de políticas nacionales, ni ninguna otra cosa y por eso DoH está en el centro de las deliberaciones porque DoH está restringido a un solo lado. Gracias.

HOLLY RAICHE: Gracias, Geoff, mucho más claro. ¿Y por qué DoH fue el tema de debate en el informe del congreso de Estados Unidos? Y quizás es lo que subyace en el comentario de La Baronesa. Me gusta el comentario de Olivier, es el caos de Paul.

Entiendo que hubo cierta discusión respecto del documento del SSAC sobre la centralización que puede darse en particular con DoH y si esto es bueno o malo o quizás pueda demorarse o generar demora.

GEOFF HUSTON: Es de conocimiento común que Chrome tiene casi el 80% de la población del internet. En el mundo de los navegadores el internet está muy centralizado, mucha gente usa el servicio de DNS público del Google y un cuarto de los usuarios envían sus queries por este. La pregunta es, ¿por qué la aplicación Chrome decidió por omisión, sin hacer referencia a nadie, enviar todas sus queries por HTTP a un resolutor recursivo de selección?

De repente todo el DNS va a un único punto de servicio y aquí la reflexión que atemoriza es que, si ese punto de extremo ya no sirve, ya no es el favorito del usuario. Más allá de la raíz esta centralización le otorga control a una aplicación dominante de un proveedor dominante y esta centralización es un mecanismo de control atemorizante que se aleja mucho de la infraestructura de un DNS alternativo, por eso esas preocupaciones.

Un único proveedor, un único operador, un único prestador tiene casi el control total de la infraestructura de nombres de dominio del internet. Chrome no ha tomado este camino, ha buscado mecanismos que permiten hacer elección o utilizar otra infraestructura, o sea es en cierta forma una preocupación hipotética, pero nos daríamos cuenta si lo hicieran, nos daríamos cuenta que están ejerciendo una operación de control nueva por omisión.

HOLLY RAICHE: Tengo un par de comentarios. Primero, como dice Olivier "un único punto de fallo". Puedo responder y Cheryl "esto de hipotético". Una pregunta… A ver si lo encuentro, de Pablo Rodríguez del consejo de la ccNSO, "parece que DoH complementa DNSSEC, ¿Cómo se puede usar independientemente de DNSSEC?"

Mi respuesta sería que es independiente del DNSSEC, pero Geoff por favor corríjame si me equivoco.

GEOFF HUSTON: Son totalmente independientes, DoH y DoT son transportes, o sea hacen la búsqueda del paquete y DNSSEC se trata de creer en lo que se

dé, uno, el usuario final. ¿Podemos confiar en lo que recibimos? Esa es la pregunta que hay que hacer en relación con el DNSSEC.

HOLLY RAICHE: ¿Podemos volver a las diapositivas 1 y 2? Ahí veremos que DNSSEC es lo que ocurre aparte del proceso de búsqueda. La siguiente.

Creo que es la siguiente, no importa. DNSSEC tiene que ver con asegurarse de que donde uno cree que va es realmente donde va, pero no se ocupa del proceso previo que es averiguar a dónde hay que ir en primer lugar. Espero que con esto haya respondido la pregunta.

¿Usted también tenía otra pregunta Gopal? No le oímos.

No estoy oyendo, usted había levantado la mano, por eso me preguntaba si quería hacer una pregunta… Bueno, ¿hay alguna otra pregunta?

Como ven, no es un tema que se preste a hacer preguntas, así que si no hay más preguntas nos quedan 10 minutos.

JOANNA KULESZA: Si miran en el chat van a ver que hay una pregunta de Bruce y también tenemos una pregunta de Vrikson, y creo que Pablo tenía algo más que una pregunta también, tenía la mano levantada.

HOLLY RAICHE: Gopal, entonces… ¿Gopal quisiera usted hacerme una pregunta o a alguien más? No lo escuchamos.

JOANNA KULESZA: Gopal podemos verlo, pero no podemos escucharlo, quizás pueda tipiar la pregunta en el chat y pasamos entonces a la pregunta de Vrikson. Vrikson puso la pregunta en el chat. "¿Qué dijo que hace Chrome y qué no ayuda? Si puede volver quizás a esa explicación Geoff y quizás dar un poco más de detalles".

Y también hay un comentario de Bruce, no sé si lo puede ver Holly en el chat…

HOLLY RAICHE: Sí, lo estoy leyendo. Geoff entonces nos da más detalles quizás sobre los navegadores o las aplicaciones. Y veo también que está la mano levantada de Olivier.

Entonces si hay una respuesta de Geoff le voy a dar luego la palabra a Olivier.

GEOFF HUSTON: La diferencia entre Chrome y Firefox en este momento. En Estados Unidos y solamente en Estados Unidos las versiones de Firefox desde octubre 2019 por defecto, sin ningún cambio en la configuración por parte del usuario empujaban las consultas del DNS/HTTPS a uno de los resolutores recursivos confiables que antes eran 1.1.1.1.

Los usuarios movieron el DNS, lo sacaron del ISP de la plataforma por defecto, Chrome tomó en cuenta esto, decidió no hacer un cambio por defecto en sí. El cambio que está contemplado en Chrome es mirar los resolutores que en ese momento están configurados dentro del sistema

operativo y que provee el proveedor de ISP y ver si esos resolutores podían dar respaldo al HTTPS.

Entonces la actitud no es cambiar cómo resolver los nombres de DNS, sino que el cambio está soportado, si se utilizan los mismos resolutores en un canal encriptado. Firefox en Estados Unidos y no en otros lados puso un comportamiento por defecto para sacar el DNS y moverlo hacia los resolutores. Esa es la distinción fundamental que yo quería mencionar.

HOLLY RAICHE: Sí, quería agradecerle a Bruce, voy a leer el comentario para que la gente sepa. “Dado que hay algunos gobiernos que están buscando dirigir los ISP en su país para que bloqueen el acceso al DNS, eso es en Australia también, quiero saber si esto va a hacer que los usuarios estén más confiables con las soluciones DoH, donde les parece que pueden perder el control.

Puedo imaginarme, por ejemplo, que la gente puede utilizar distintos navegadores para distintos objetivos. Por ejemplo, un navegador para trabajador, otro para acceder a cosas como shows de televisión, etc., y que quizás no estén disponibles en un país en particular.

De hecho, exactamente de eso se habla en una de las diapositivas de Paul, creo que es el paper del OCTO. Creo que es parte del SSAC, pero no estoy seguro. Geoff, ¿esto fue parte de SSAC? Es decir, la posibilidad de que se utilicen distintos navegadores para distintos objetivos…”

GEOFF HUSTON: No distintos navegadores, pero, si uno amplia un poco su mente, hay distintas aplicaciones que van a distintos lugares, por supuesto, que esto es una pesadilla. Imagínense que DNS es lo mismo en todos lados, es decir, yo hago una pregunta u otro hace una pregunta y es la misma respuesta, pero tratar de verificar algo con una aplicación diferente y tener una respuesta diferente, ahí es donde todos nos empezamos a confundir.

Yo creo que este es el argumento que respalda la tesis de que el DNS se está fragmentando y que está saliendo de control, está habiendo caos como se dijo antes. Gracias.

HOLLY RAICHE: Gracias, Geoff. ¿Quisieran hacer algún comentario?

OLIVIER CRÉPIN-LEBLOND: Le voy a dar la palabra a Pablo, que me parece que hace mucho que está esperando, y luego voy a hacer mi pregunta después de él, si les parece bien. Pablo adelante, por favor.

PABLO RODRÍGUEZ: Muchas gracias, Olivier y Holly, por las excelentes respuestas. Tengo una pregunta sobre la implementación de ambos protocolos.

Parece que sobre la base de las distintas configuraciones serían menos difíciles implementarlo y también, ¿uno está más seguro si implementa DNSSEC, DoT y DoH? Gracias.

HOLLY RAICHE: Bueno, Pablo no estoy muy segura, pero si pensamos en implementar ambos no se me ocurre muy bien si podemos implementar DoH y DoT.

GEOFF HUSTON: No hay que olvidarse que hay distintos lugares y DoH en general, es un paquete que está dentro de la aplicación, no se le puede poner por separado. Yo sé que Cloudflare tiene un paquete para la laptop, pero eso es algo bastante raro, es decir, que no es algo que uno como usuario puede instalar y configurar.

La aplicación que uno está corriendo podría tenerlo incluido o no, pero ahí es donde está la responsabilidad de las aplicaciones. DoT es algo que uno normalmente instala como un driver y ciertamente requiere trabajo práctico, hay que conocer […] pero es un poco raro, las dos se implementan del mismo modo. Todos utilizan la plataforma de transporte de seguridad en general, utilizan SSH o alguna librería y pueden también utilizar TLS o algunos de los otros.

Pero lo que encapsula HTTPS o DNS no hace mucha diferencia, como codificador el trabajo es el mismo para ambos, como codificador entonces se ve bastante parecido. Es la misma capa de encapsulación que la que hay en TLS porque la librería llama al TLS.

DNSSEC es completamente distinto, es parte del código de resolución en la librería de DNS, no es parte de la misma técnica y también podría utilizar HSS abierta para la criptografía, pero eso es una librería de criptografía general. DNSSEC entonces es distinto de DoT y DoH porque DoT y DoH utilizan el mismo substrato para dar seguridad, lo que es distinto es lo que lo encapsula.

Y también, como decía antes, la falta del control. DoT es parte de un sistema operativo como decimos y DoH es un paquete que está dentro de las aplicaciones y allí es donde está el asunto.

HOLLY RAICHE: Gracias, Geoff. Joanna, ¿tenemos alguna otra pregunta? Porque seguramente nos vamos a pasar.

JOANNA KULESZA: Tenemos la mano levantada de Olivier y veo también una pregunta de Gopal en el chat. Y vamos a pedirles a nuestros participantes que hagan la encuesta, así que sugeriría que tomemos el comentario de Olivier, a que él tenga la palabra.

Y quiero alentar a todas las otras preguntas que tengan para hacer que la manden por email, tenemos el acuerdo de nuestros intérpretes para extender la reunión 5 minutos más y si les parece bien a los participantes les vamos a pedir que se queden unos minutos más para el cierre breve.

Vamos a escuchar entonces ahora a Olivier y tiene también la mano levantada Pablo, puede tomar la palabra Pablo también. Y les pido entonces que las preguntas las manden por correo.

HOLLY RAICHE: Sí, creo que está muy bien. Cualquier pregunta adicional las vamos a responder por email.

Joanna, ¿podría tipiar en el chat a qué dirección se pueden enviar las preguntas?

JOANNA KULESZA: Les voy a poner el Dashboard, el tablero de control de generación de capacidad…

HOLLY RAICHE: Le voy a dar la palabra a Olivier.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Holly, es una pregunta en realidad. Estuvimos escuchando lo que nos preocupa mucho, que es toda esta concentración del control, del poder potencialmente. Para mí esto se traduce en algo menos recibiente y algo menos reciente se convierte en un Blackout, en una oscuridad, como que las redes desaparecen por un momento, se apagan por un momento.

Y como sabemos, los proveedores de computación en nube; que prefiero no mencionar los nombres, aparecen offline por razones que no se pueden explicar y aparecen errores, etc. ¿Hay alguna forma de contrarrestar esto a través de una multiplicación de proveedores de DoH? ¿Hemos encontrado alguna manera de contrarrestar esta parte, esta pérdida de resiliencia?

GEOFF HUSTON: No, perdón.

HOLLY RAICHE: Gracias, Geoff, es como mi socio de la presentación, Geoff. Y Joanna entonces te voy a dar la palabra para que respondamos las preguntas, primero les voy a agradecer a todos por haber asistido, le agradezco a Geoff Huston, a APNIC y le doy la palabra a Joanna.

JOANNA KULESZA: Gracias por esta impresionante presentación y gracias, Geoff, por participar también, y a todos los demás por unirse. Agradezco a la parte de gobierno y de seguridad que ha habido, le quiero agradecer a los miembros del GAC que veo entre la lista de los participantes.

Quiero aprovechar esta oportunidad para recordar que trabajamos junto con el GAC. Antes de cerrar y les voy a dar detalles sobre cómo involucrarse con este webinar, le voy a dar la palabra a Gisella para que nos cuente cuál es la encuesta que hacemos al final de cada webinar para que podamos nosotros así saber qué les gustó y qué no y mejorar nuestros próximos seminarios web. Gisella, por favor.

GISELLA GRUBER: ¿Pueden ponerla en la pantalla? La encuesta en la pantalla… No, no podemos verla. ¿Pueden verla ahora?

JOANNA KULESZA: Ahora sí está.

GISELLA GRUBER: Muy bien, vamos a leer las preguntas. La uno, ¿cómo se enteraron de este seminario web? Las opciones son: Twitter, Facebook, Email de At-

Large, calendario de At-Large, Skype, un colega u otro. Les voy a dar unos segundos más.

Esperemos que muchos participen. Judith, ¿usted ha probado elegir más de una respuesta?

JOANNA KULESZA: No sé si a encuesta lo permite en este punto, pero seguramente este sería un buen cambio, así que lo podemos incorporar. En este punto, por favor elijan el que les llegó primero, pero como Judith dijo, le agradecemos por la pregunta, ¿no? Elegir más de una opción.

GISELLA GRUBER: Por favor, tengan un poquito más de paciencia hasta que lleguemos a la pregunta número 2. Pido disculpas, pareciera que aquí hay un asunto técnico, un problemita técnico con esta encuesta.

JOANNA KULESZA: Quiero invitar a nuestros participantes a que se unan a otro webinar que va a haber en dos semanas, dado que vamos a estar ya cerca de nuestra próxima reunión de la ICANN…

Veo, Gisella que está la pregunta número 1 que aparece en la pantalla.

GISELLA GRUBER: Sí, esta es la pregunta 1 y la número 2 parece que no quiere aparecer. De nuevo, pido disculpas por este problema técnico.

JOANNA KULESZA: Quizás lo que podemos hacer es cerrar y vamos a trabajar en la encuesta para estar seguros de que esté disponible la próxima vez en el próximo webinar. ¿Les parece bien?

HOLLY RAICHE: Sí, está bien, me parece bien.

JOANNA KULESZA: Bueno, entonces voy a cerrar Gisella y vamos a tratar de recibir el feedback por otros canales. El próximo webinar va a ser presentado por Jonathan Zuck, estamos ya acercándonos a la reunión de ICANN69 y queremos invitarlos a que nos cuenten sobre su experiencia con las reuniones remotas virtuales y cómo hacer para que mejoren.

El próximo seminario web que estoy poniendo en el chat se va a focalizar en dar mejores presentaciones, de cara a ICANN69, todos están invitados y nos encantará que participen el día 22 de septiembre. Esta vez el horario va a ser menos amigable para Australia, va a ser a las 20:00 UTC, yo coloqué el link en el tablero de control de generación de capacidades, allí pueden ver todas las próximas reuniones.

Y vamos a tratar de que estas reuniones sean lo más útiles posibles. Ahora sí, entonces voy a cerrar, les voy a agradecer a nuestros oradores del GAC, le agradezco a Holly y a Geoff por todos estos ejemplos prácticos y útiles, y también por sus comentarios y observaciones.

Gracias por participar. Como dije, este es un ejercicio intercomunitario. También le agradezco a Alfredo, mi copresidente del grupo de generación de capacidad, a nuestro personal: no lo podríamos hacer sin

ustedes, y también a los intérpretes que hacen que este sea un acontecimiento multicultural. Que tengan un buen día, buenas tardes y buenas noches.

[FIN DE LA TRANSCRIPCIÓN]