GISELLA GRUBER : Bonjour, bon après-midi et bonsoir. Bienvenue [inaudible, coupure audio pour les premières deux minutes].

Nous n'allons pas faire l'appel nominal pour cet appel. Les présences seront notées sur [inaudible].

[inaudible] ainsi que pour la transcription. Nous avons également la transcription en temps réel. Le lien est affiché sur l'ordre du jour et je vais également le mettre dans le chat.

Veuillez parler à un rythme raisonnable [inaudible].

Merci de votre attention. La parole est à Joanna.

JOANNA KULESZA : Merci beaucoup Gisella.

Bienvenue à ce webinaire sur un aspect technique du DNS et sur la gouvernance de l'internet. Nous avons des acronymes que la communauté At-Large connaît bien. Et nous avons une excellente intervenante, Holly Raiche, pour parler de ce thème aujourd'hui. Nous avons donc quelqu'un qui connaît bien la gouvernance de l'internet, le DNS et toutes ces problématiques et qui a beaucoup enseigné en Australie et en dehors de l'Australie.

Vous avez notre ordre du jour et vous y voyez que je vais essayer d'être très brève. Nous n'avons que cinq minutes. Nous avons 30 minutes pour la présentation de Holly et ensuite, nous aimerions vous entendre avec

vos questions sur ce DoH et ce DoT. Nous aurons une vingtaine de minutes pour répondre aux questions. Nous aimons beaucoup l'interactivité. Si vous avez l'opportunité de prendre la parole, n'hésitez pas à le faire, à lever la main donc, et nous vous donnerons la possibilité de prendre la parole avec le micro. Si vous voulez poser des questions après la présentation ou instantanément, vous pouvez utiliser le chat pour poser de questions également comme vous pouvez le voir à l'écran.

Nous allons également vous demander un retour sur ce webinaire. Nous essayons toujours de répondre au mieux aux intérêts de nos auditeurs. Nous voulons savoir si on a répondu à vos questions, à vos besoins, ou si nous pouvons améliorer quoi que ce soit. Mais sans plus attendre, je devais donner la parole à Holly Raiche. Nous la remercions d'avoir accepté notre invitation pour éclairer un petit peu ces acronymes. Vous voyez DoH, DoT. Holly, dites-nous-en plus sur ces acronymes et les politiques qui sont derrière tout cela et l'intérêt pour les utilisateurs finaux. Merci beaucoup une nouvelle fois.

HOLLY RAICHE : Merci beaucoup.

On pourrait en dire beaucoup sur ces sujets. Je n'ai pas de petit test aujourd'hui pour vous parce qu'il y a beaucoup de choses à dire sur ces questions un petit peu techniques. Les spécialistes de l'internet se penchent sur la question. Je ne suis pas une spécialiste technique de l'internet. Mais nous avons Geoff Huston qui a écrit des articles à ce sujet et qui va très loin au niveau technique et technologique. Geoff est

membre en Australie du groupe spécialisé. Moi, je vais essayer de prendre une approche non technique.

Nous avons des questions sur les utilisateurs finaux, sur la gouvernance et sur la manière dont l'internet fonctionne. Voilà ce dont je vais parler. Je ne vais pas prendre plus de 30 minutes. Mais les questions de terminologie se posent, donc définir ces termes de base, comment cela fonctionne-t-il, quels sont les processus qui sont utilisés pour ces technologies, quels sont les inconvénients et comment pouvons-nous avancer avec ces protocoles.

Pour beaucoup d'entre vous, vous allez aux réunions de l'ICANN et il y a des séances spécialisées sur ces thèmes. Elles sont souvent très techniques. Et lors de la dernière réunion présentielle de l'ICANN, nous avions parlé de cela.

En mars, nous avons eu une réunion virtuelle également sur le DoH et le DoT. Je ne m'attends pas à ce que vous soyez tous familiers avec ces termes. Je vais donc poser quelques questions à Geoff. Commençons avec la première diapositive.

Il y a des termes de base à connaître. Je crois que vous savez comment fonctionne l'internet pour la plupart d'entre vous, mais quelques petits rappels. Nous allons voir dans quel contexte et avec des diagrammes comment cela fonctionne au niveau des messages du DNS.

À la base, il y a un protocole de requêtes et de réponses ; c'est cela le DNS. Vous utilisez un navigateur, vous tapez sur votre ordinateur et cela, c'est envoyé en tant que requête DNS sous forme de protocole

internet IP et cela va être des chiffres. Et cela passe d'un ordinateur à un autre sur le DNS. Voilà un des termes dont on parle.

Les noms de domaine sur la sécurité de la couche de transport ou TLS, c'est un protocole qui a pour but de fournir un respect de la vie privée, une intégrité des données. La couche de sécurité, de transport, fait circuler des paquets par l'intermédiaire du DNS entre mon ordinateur vers d'autres navigateurs et d'autres ordinateurs.

Le DoH, vous devez le savoir. Le HTTPS, vous le connaissez, ce sont des protocoles sécurités des transferts hypertexte, HTTPS. DoH, c'est le DNS sur le HTTPS qui est un protocole utilisé pour envoyer des données entre un navigateur et un site web. Là aussi, c'est quelque chose qui sécurise les données qui passent d'un endroit à un autre sur l'internet.

Nous avons une présentation de Paul Hoffman qui a déjà beaucoup parlé de cela et qui a parlé de boîtier intermédiaire, *middle box* en anglais, d'un système qui peut éventuellement modifier le trafic. C'est un système sur le réseau entre le client et un serveur.

Ces boîtiers intermédiaires peuvent servir de pare-feu, ils peuvent servir de filtre également. Ces boîtiers intermédiaires, c'est quelque chose d'intermédiaire entre vos paquets d'informations qui demandent où aller et quand ces paquets d'informations se lancent dans leur voyage, si je peux m'exprimer ainsi, sur l'internet. Passons à la diapositive suivante.

J'espère que vous pouvez voir le diagramme sur la gauche ; cela explique un petit peu. Si vous regardez sur ce diagramme, je tape une adresse, par exemple atlargeicann.org/alac, cela est envoyé à un

résolveur et ces paquets vont être envoyés de cette manière à cette adresse.

Le paquet commence à partir du résolveur. Vous avez le serveur racine qui est utilisé et la question qui est posée, c'est « Où voulez-vous vous diriger ? Vers quelle adresse IP ? » Vous devez aller au DNS.

Maintenant que j'ai cette information, je sais où je dois aller, vers ICANN. Et je sais où je dois retourner, At-Large. Donc on a une réponse qui est envoyée pour avoir cette adresse IP qui est une série de numéros qu'on me renvoie et on dit : « D'accord. Maintenant qu'on a la carte de notre objectif, on y va. »

Ces voyages sont en rouge pour vous montrer qu'ils ne sont pas chiffrés. C'est là où se trouve le problème, dans ce domaine, dans cette partie qui n'est pas chiffrée et qui nous préoccupe. Ce voyage, lorsqu'on envoie notre paquet d'informations, cette partie peut être chiffrée, le système de recherche DNS ne l'est pas. Et on a toute une série de possibilités qui peuvent arriver ici dans le domaine de la protection des enfants, de l'utilisation malveillante du DNS, etc. Prochaine diapositive. Est-ce que je peux avoir la prochaine diapositive s'il vous plaît ?

Récemment, on a attiré l'attention du public sur la partie du système classique de recherche parce que c'est une partie du processus qui n'est pas chiffrée. Donc même si on utilise des systèmes comme le DNSSEC ou des mesures de sécurité, ce processus n'est pas chiffré. Il laisse la possibilité à une utilisation abusive du DNS, par exemple avec la taxe de l'homme du milieu et autres problèmes, donc des problèmes de protection de la vie privée.

Tout le monde sait maintenant qu'il y a beaucoup de matériel non chiffré sur internet qui peut être utilisé et dont on peut abuser sans autorisation, si l'on demande cette autorisation ou pas. C'est donc là que toutes ces données sont connectées. L'autre problème est le fait que dans cet espace, c'est là que beaucoup de choses peuvent arriver, c'est là que les contrôles et les filtres ont lieu. On a des problèmes de protection de vie privée qui peuvent arriver à cet endroit. Prochaine diapositive.

Pour que ce soit plus clair, je dirais que les seuls changements que le DoT ou le DoH peut faire, c'est d'utiliser un transport chiffré dans ce processus de recherche, non pas changer la requête ou la réponse ou tout autre changement de protocole. Ici, il faut chiffrer d'une manière ou d'une autre ce qui n'est pas chiffré. Prochaine diapositive s'il vous plaît.

On revient à l'époque de 2016, lorsqu'on a commencé à prendre conscience de ce problème, des bonnes choses et des mauvaises choses qui pouvaient avoir lieu à cause de ce processus de recherche lié au DNS non chiffré. Que se passe-t-il lorsque des chiffrements du TLS n'ont pas lieu ? On a un système de DNS qui est entre l'ordinateur de l'utilisateur final et le résolveur récursif, c'est là que cela arrive. C'est la partie du transport. Est-ce que je peux avoir la prochaine diapositive s'il vous plaît ?

Ce que vous voyez ici, c'est une illustration de ce que peut être ce processus de recherche du DNS pour le réseau dans sa totalité. Ici, vous voyez la partie chiffrée, vous voyez l'ordinateur. Ce qui est en rouge est la partie chiffrée, c'est l'ensemble du processus du résolveur. Vous

voyez la partie non chiffrée. Et on a cette connexion. Prochaine diapositive.

Maintenant, voyons un réseau d'entreprises. C'est là que le chiffrement a lieu de nouveau. Encore, ce n'est pas chiffré et la connexion entre l'endroit dont on vient et l'endroit où on va est rompue ici au niveau de la flèche rouge, c'est-à-dire au niveau du résolveur minimum. Prochaine diapositive.

Le DoH est un petit peu plus sophistiqué. C'est la dernière version d'un système qui permet d'ajouter de la protection à la vie privée dans ce processus de recherche. Et de nouveau, ici, le message est transporté sur le TLS. Donc on voit qu'il y a davantage de protection et de chiffrement qui permet au serveur de pousser les réponses DNS avant qu'elles soient requises. Le DoH est donc conçu pour chiffrer le trafic du DNS pour les applications.

Il y a un autre point important ici dans le document du SSAC qui se trouve sur le site internet du SSAC, le SSAC109 qui a été présenté et publié lors de la réunion du mois de mars cette année, qui montre comment les transactions du DNS ont lieu. Le TLS va transformer ces paquets et comme la transaction actuelle a lieu sur le HTTPS, il y a eu beaucoup de difficultés au niveau gouvernemental à propos de ce point-là. Il y a eu des documents qui ont été présentés, il y a eu des débats. On parle de DoH. Et tout cela au niveau des requêtes du DNS, non pas au niveau des tierces parties. Et c'est là qu'il y a des questions de manque de protection de la vie privée, manque de données, des questions de violation de la sécurité, etc. Prochaine diapositive.

Ici, vous voyez que la flèche rouge est beaucoup longue dans ce diagramme. Ici, on a le DNS tout au long de la couche de transport jusqu'au fournisseur internet ou au nuage. Donc on a davantage de sécurité quand on a ce déploiement de HTTPS. On a un processus qui va accompagner le système jusqu'au résolveur récursif en partant de votre navigateur. Prochaine diapositive.

Voyons les différences entre DoT et DoH. DoT peut être identifié et bloqué et c'est important de voir que c'est ce qui peut arriver au niveau de votre fournisseur d'internet. Cela peut aussi bloquer d'autre trafic. Donc d'un côté, c'est plus sûr mais cela donne lieu à d'autres problèmes aussi. Prochaine diapositive.

J'aime beaucoup cette citation de la baronne de Thornton, lorsqu'elle s'est adressée à la chambre des Lords en Angleterre. Elle s'inquiète à propos d'une question concernant le DoH et elle pose une question au gouvernement, quelque chose qui inquiète les gouvernements, il s'agit de la responsabilité de l'IETF, les personnes qui sont employées par les grandes compagnies qui gèrent l'internet. Cela peut avoir de grandes conséquences pour nous tous et elle demande quelle est la responsabilité du gouvernement anglais par rapport aux compagnies qui gèrent l'internet et qui représentent l'IETF. Elle souligne donc le problème concernant la responsabilité des gouvernements par rapport à ce qui se passe. C'est le grand débat qui a lieu actuellement en Angleterre. On a beaucoup de discussions à propos de l'impact que la technologie peut avoir en général sur les utilisateurs finaux. Prochaine diapositive.

Ces deux systèmes, DoT et DoH, pourquoi est-ce qu'on doit faire cela ? C'est une question de protection de la vie privée. Vous, en tant qu'individus, vous devez vous rendre dans un endroit qui est chiffré. Il n'y a pas de connexion entre vous et le résolveur récursif pour le DoT alors que pour le DoH, ce voyage, cette recherche va se faire sur le HTTPS. Dans les deux systèmes, la connexion va être interrompue.

Quels sont les avantages ? Si on a le système de recherche classique, les requêtes du DNS peuvent être interceptées pour manipuler le trafic légitime. Et le résultat sera des problèmes de sécurité. Les services peuvent ne pas être disponibles, les informations que vous avez envoyées peuvent être collectées au passage et d'autres activités malhonnêtes appartenant aux catégories de l'utilisation malveillante du DNS peuvent être réalisées. On peut prévenir cela au niveau de la sécurité. L'usurpation et ainsi de suite peut être évité. Il y a des processus pour cela. Prochaine diapositive.

La raison pour laquelle je n'ai pas de quiz, de petites questions, c'est qu'il n'y a pas de réponse facile. Qu'est-ce qu'il y a de mieux ? Il y a des bons aspects et des aspects beaucoup plus négatifs. Les prestataires de service peuvent avoir des pare-feu. Petit problème technique, excusez-moi. Voilà, vous avez la diapositive à nouveau à l'écran.

Vous pouvez éviter que des courriels envoient des logiciels malveillants. Et les prestataires de service internet peuvent éviter la communication avec des serveurs ayant une utilisation malveillante du DNS après avoir été infectés. Les gouvernements peuvent demander le blocage des sites, les parents ont des contrôles pour protéger contre certains sites. Mais si vous bloquez le trafic de cette manière, il y a beaucoup de

gouvernements et notamment, le gouvernement Australien filtre parfois.

Ce qui peut se passer également, c'est que beaucoup d'entreprises ont des informations sensibles, donc observent le trafic. Ils peuvent voir quel type de matériel ou de document part et les entreprises peuvent avoir des mesures de sécurité à ce niveau.

Mais cela peut être également utilisé pour limiter les communications de certains groupes dissidents et on peut accéder à des informations sur tous les sites qui sont visitées. Donc vos informations personnelles peuvent être visibles. Et on ne veut pas que ces informations tombent dans de mauvaises mains. Je dirais qu'il y a des avantages et des inconvénients au filtrage. Passons à la prochaine diapositive. Très bien.

Les avantages, nous les avons vus. Il y a peut-être des caches plus importantes avec des réponses plus rapides – ce sont des avantages – et configuration plus aisée. Tout cela provient du SSAC. Si le trafic est envoyé uniquement aux résolveurs choisis de l'ISP, du prestataire de service internet, là, c'est beaucoup plus étroit et les paquets ne peuvent aller que là. Là, il doit y avoir des cibles avec des mauvais acteurs, avec des attaques de déni de service notamment avec des actions malveillantes. Et étant donné qu'il y a moins d'endroits où le paquet peut aller, il y a la possibilité d'avoir un trafic plus lent au niveau de l'internet. Une nouvelle fois, vous avez de avantages et des inconvénients à cette centralisation de la résolution du DNS.

Très bien. Où en sommes-nous ? Si vous utilisez Firefox, ils ont un programme TR de résolveur récursif de confiance. Ils utilisent CloudFlare et NextDNS comme parties de leur programme. Ils n'utilisent

pas le processus normal pour le DNS et ils utilisent leur propre résolveur de confiance.

En ce qui concerne Google Chrome, il y a des tests qui sont effectués. Microsoft commence à réfléchir à cela. C'est quelque chose dont on parle beaucoup en ce moment. Sur mon ordinateur, j'utilise Firefox Mozilla, donc c'est en train de se passer en temps réel pour moi sur mon ordinateur avec Firefox.

Par rapport à l'article de Paul Hoffman, quelles sont les solutions ? Au niveau des boîtiers intermédiaires, il est possible que l'on puisse préserver l'anonymat mais il y a également des contrôles de boîtier intermédiaire. C'est là où se situe la protection, c'est là où il y a les contrôles parentaux notamment, c'est là où il y a le filtrage. Donc il se peut qu'on puisse s'éloigner un petit peu du DNS classique et qu'on puisse garder les avantages du DNS classique, mais vous avez toujours ces boîtiers intermédiaires qui existent entre une adresse IP et une autre. Il y a des possibilités que ce trafic internet chiffré soit du trafic DNS et qu'on puisse préserver les aspects positifs, les filtres par exemple qui sont positifs pour le respect de la vie privée.

Je crois que je suis bientôt à la fin de ma présentation. Voici ma dernière diapositive, des liens de référence concernant cela. On en a parlé lors de deux réunions avec Paul Hoffman le 12 mars 2019 et le 10 mars 2020, on en a parlé également lors de ces réunions de l'ICANN. Cela est disponible sur l'internet sur le site de l'ICANN. L'article de Paul Hoffman est également sur le site web de l'ICANN. Vous avez donc l'article du SSAC109. Vous avez également le service de recherche du Congrès des États-Unis qui a travaillé là-dessus. Vous avez l'adresse à l'écran, donc

vous pouvez vous informer de cette manière. Commencez peut-être avec l'article du SSAC.

Voilà pour ma présentation. Il nous reste 20 minutes pour toute question que vous pourriez avoir à ce sujet. J'espère que je n'ai rien oublié ; ce serait ma première question. Nous pouvons regarder sur le chat s'il y a des questions. Geoff ?

GEOFF HUSTON : Merci Holly. C'était une explication très claire.

Je m'appelle Geoff Huston et je suis avec APNIC.

Il y a une différence entre DoH et DoT. C'est l'endroit où il y a le contrôle. Le DNS, c'était l'ISP qui le dirigeait beaucoup et vous aviez un système opérationnel. Avec quelque soit l'application que vous utilisiez, toutes les requêtes passaient par le même protocole, passaient par le système d'opération et étaient résolues de cette manière.

Avec DoT sur le TLS, cela change un petit peu les choses. DoT, c'est un protocole de transport, comme on l'a vu. Et les applications se préoccupent beaucoup moins du DNS qui est un petit peu mis de côté avec DoT. Donc d'une certaine manière, avec cette sécurité de la couche de transport, c'est différent.

DoH a eu beaucoup de réactions parce que cela, c'est au niveau des applications. On peut voir Mozilla et Firefox, je peux avoir tout type d'application. Et cette application peut choisir de faire des requêtes DNS en utilisant ses résolveurs préférés sans référence à toute autre

application sur votre appareil. Maintenant, vos requêtes vont pouvoir apparaître partout.

Et la solution proposée par Paul Hoffman d'avoir des boîtiers intermédiaires pour avoir un système de sécurité, c'est un petit peu antithétique par rapport aux pratiques de sécurité. Les boîtiers intermédiaires ne fonctionnent pas très bien de cette manière, on ne peut pas leur faire confiance. Ce type de solution peut être [inaudible].

Ce qui se passe ici et le problème à régler, c'est que maintenant, le DNS n'est plus limité par des canaux bien compris. Les applications ont la possibilité de gérer la manière qu'ils choisissent ces requêtes DNS. Il n'y a plus de politiques nationales, il n'y a plus rien qui compte. Et cela, véritablement, c'est pour cela que DoH, on en parle beaucoup, parce que DoT, c'est tout simplement un système de transport.

HOLLY RAICHE : Oui, c'est beaucoup plus clair et c'est pour cela je pense que c'est DoH, DNS sur HTTPS, qui fait l'objet de plusieurs rapports. Et c'est ce dont parlait cette baronne anglaise.

J'ai vu le commentaire d'Olivier. Oui, cela s'appelle le chaos.

Je vois qu'on a parlé également de l'article du SSAC et de la centralisation, particulièrement dans le cadre de DoH. Est-ce une bonne chose ou pas ? Est-ce que ces messages vont passer ? Est-ce qu'il va y avoir un système de...

GEOFF HUSTON : Très rapidement, une nouvelle fois.

Avec Chrome, beaucoup de personnes utilisent Chrome. Là, l'internet est très centralisé. [25 %] des utilisateurs font des requêtes en utilisant Google – c'est beaucoup. Mais le scénario est le suivant. Si Chrome décidait par défaut de ne plus faire référence à qui que ce soit et d'utiliser HTTPS, ce ne serait plus blocable, donc ils pourraient utiliser les résolveurs de leur choix. À ce moment-là, tout le DNS arriverait à un seul point de service. Et ce qui se passerait, c'est que si ce point de service ne répondait pas bien à .com, quelle que soit la racine, quel que soit le DNS, le nom de domaine ne fonctionnerait plus et la centralisation poserait problème. Il y aura une application dominante qui aurait un contrôle beaucoup plus important Donc la centralisation, c'est un mécanisme de contrôle qui est inquiétant alors que maintenant, nous avons une structure de délégation au niveau du DNS. C'est pour cela qu'il y a beaucoup de préoccupations au niveau de la centralisation. Un seul opérateur, un seul prestataire de service qui a une importance très grande sur la gestion de l'internet. Et cela, c'est une possibilité qui peut arriver. Chrome n'est pas encore à ce niveau. Chrome a toujours des mécanismes qui vont fournir un certain degré de choix pour la structure du DNS, donc ce dont je parle est hypothétique mais c'est une possibilité avec le temps qui pourrait exister. Est-ce que vous seriez conscient de cela ou pas ? Non, nous ne le serions pas. Donc véritablement, sans qu'on s'en rende compte, cela peut arriver.

HOLLY RAICHE : Merci beaucoup Geoff.

J'ai quelques commentaires. Olivier nous parlait d'un point unique d'échec et de l'aspect hypothétique des choses.

Une question de Pablo Rodriguez du conseil de la ccNSO : « Comment est-ce qu'on peut utiliser cela indépendamment du DNSSEC ? » Ma réponse serait que cela est indépendant du DNS. Mais Geoff, s'il vous plaît, corrigez-moi si je me trompe.

GEOFF HUSTON : Ils sont tout à fait indépendants. DoH et DoT sont des transports. Le DNSSEC concerne la conviction que ce l'on entend est juste. « Est-ce que l'on peut faire confiance à cela ? », c'est la question que pose le DNSSEC.

HOLLY RAICHE : Si vous revenez aux diapositives précédentes, la première ou la deuxième, vous voyez que le DNSSEC, c'est ce qui se passe au niveau du processus de requête ou de recherche. Prochaine diapositive s'il vous plaît. Je crois que c'est la prochaine. Le DNSSEC, c'est de vous assurer que votre objectif sera vraiment atteint. Mais il y a un processus avant cela qui est de trouver où vous allez en premier lieu. J'espère avoir répondu à votre question.

Gopal, vous avez la main levée ? Vous avez une question à poser ? Gopal, on ne vous entend pas. On n'entend rien, Gopal. Vous avez la main levée, donc je pensais que vous vouliez poser une question, mais nous ne vous entendons pas.

Est-ce qu'il y a d'autres questions ? Normalement, il y a un quiz qui va arriver après s'il n'y a pas d'autres questions.

JOANNA KULESZA : Je vois dans le chat que nous avons un commentaire de Bruce puis une question de Vrikson. On peut peut-être demander à Pablo s'il a autre chose à ajouter.

HOLLY RAICHE : Gopal, est-ce que vous voulez poser une question à moi-même ou à Geoff ? Vous êtes en muet ? Joanna, je n'entends pas Gopal.

JOANNA KULESZA : Gopal, on ne vous entend pas. Si vous voulez, vous pouvez poser votre question dans le chat et à ce moment-là, nous y répondrons.

On va prendre la question de Vrikson en attendant : « Qu'est-ce qui a été dit que Chrome ne possède pas ou sur quoi ils travaillent ? »

Ensuite, nous avons un autre commentaire de Bruce.

HOLLY RAICHE : Je suis en train de le lire.

JOANNA KULESZA : Geoff, est-ce que vous pouvez faire une différence entre le navigateur et l'application qui pourrait répondre aux questions qui ont été posées ? Je vois qu'Olivier a aussi la main levée. Donc Geoff, si vous avez une réponse. Ensuite, peut-être que nous donnerons la parole à Olivier et à Pablo.

GEOFF HUSTON : Je vais répondre rapidement à la différence entre Chrome et Firefox.

Aux États-Unis et seulement aux États-Unis, Firefox, depuis le mois d'octobre 2019, il n'y a pas de changement dans la configuration et cela envoie les requêtes du DNS sur HTTPS. Je crois que c'était Cloudflare 1.1.1.1.

Les utilisateurs ont dû déplacer leur DNS par défaut. Et Chrome a analysé cela et a décidé de ne pas faire cela, de ne pas faire un changement par défaut. Et l'attitude de Chrome est d'analyser les résultats qui ont lieu actuellement qui sont configurés dans le système opérationnel et de voir si ces résolveurs peuvent supporter le système. Donc Chrome a décidé de ne pas savoir qui allait résoudre le nom du DNS, mais c'était de voir si cela allait être soutenu si on utilisait le même résolveur. Firefox aux États-Unis seulement a changé ce comportement.

C'est la différence importante qui existe actuellement. Merci.

JOANNA KULESZA : Merci beaucoup.

HOLLY RAICHE : Je voulais remercier Bruce. Je suis en train de lire le chat. Je vois ici la possibilité de filtrer l'accès au DNS pour être plus à l'aise avec une solution de DoH. J'imagine par exemple qu'il y a des personnes qui pourraient utiliser différents navigateurs pour différents objectifs, par exemple un navigateur pour le travail et un autre navigateur pour accéder à certaines choses comme par exemple un film qui n'est pas disponible dans un pays. De fait, je crois c'est dans un document d'OCTO dont on a parlé de cela. Je pense que c'était une partie du SSAC, la possibilité d'utiliser différents navigateurs pour différents objectifs.

GEOFF HUSTON : Pas différents navigateurs, mais différentes applications utilisées de différentes manières. Cela donne lieu à un cauchemar parce qu'on disait que le DNS était le même partout. On pose une question au nom de domaine, on a une réponse qui est toujours la même. Mais dans le domaine des applications, ce n'est pas le cas. On peut utiliser d'autres applications et avoir différentes réponses. À ce moment-là, il y a une grande confusion. Je pense que c'est un argument pour soutenir le fait que le DNS est fragmenté et que cela devient hors contrôle, cela devient un chaos comme l'a dit Olivier tout à l'heure.

Merci.

HOLLY RAICHE : Merci Geoff.

Olivier, est-ce que vous voulez faire un autre commentaire ?

OLIVIER CRÉPIN-LEBLOND : Oui, merci Holly. Je voulais donner peut-être la parole à Pablo d'abord parce que je crois que cela fait un moment qu'il attend et ensuite, je prendrai la parole.

HOLLY RAICHE : Pablo, allez-y alors.

PABLO RODRIGUEZ : Merci Olivier. Merci Holly et Geoff pour ces bonnes réponses.

Ma question porte sur la mise en œuvre de ces deux protocoles, leur déploiement. Il semble qu'en fonction des différents réglages qu'on peut avoir, on a des résultats différents.

Et aussi, je voulais savoir, si on a une connexion à travers le DNSSEC via DoH ou DoT, que se passe-t-il ?

HOLLY RAICHE : Merci.

Geoff, est-ce que vous pensez qu'on peut implémenter ces deux systèmes, le DoH et le DoT ?

GEOFF HUSTON : N'oubliez pas que dans certaines situations, il y a différents lieux. Le DoH fonctionne dans les applications. Il peut être ajouté séparément. Je sais qu'il y a un paquet de DoH qu'on peut utiliser sur un appareil portable, mais il est rare qu'un utilisateur utilise et installe ce type de configuration. En général, l'application l'a ou ne l'a pas, mais cela dépend de la responsabilité de l'application. En général, on va installer les *drivers*. C'est un système très rare. Tous les deux sont implémentés de la même façon et vont utiliser la plateforme de sécurité de couche de transport. Et ils peuvent aussi utiliser différents systèmes.

L'encapsulement du TLS, que ce soit sur le DNS ou pas, ne fait pas de différence. Donc la quantité de travail est la même pour les deux. Pour un codeur, c'est plus ou moins la même chose et il y a en général un encapsulement.

Le DNSSEC est complètement différent. Cela fait partie du code de résolution dans votre bibliothèque DSN. Ce n'est pas la même technique. Donc on peut faire un chiffrement mais de nouveau, je dirais que c'est seulement une bibliothèque de chiffrement. Donc le DNSSEC est différent en fonction du DoH ou du DoT et au niveau de la sécurité.

La principale différence est le locus du contrôle. DoT fait partie d'un système opératif. DoH est à l'intérieur des applications et c'est là que se trouve le problème.

Merci.

HOLLY RAICHE : Merci Geoff.

Est-ce que nous avons d'autres questions ? Il nous reste deux minutes, c'est tout.

JOANNA KULESZA : Merci Holly.

Nous avons un commentaire d'Olivier. Je vois aussi une question de Gopal dans le chat. Et nous allons demander à nos participants de répondre à l'enquête. Donc on peut peut-être donner la parole à Olivier. Ensuite, toutes les questions qui sont posées pourront être envoyées à la liste de diffusion de notre groupe de travail. Les interprètes peuvent prolonger la réunion de cinq minutes. Donc nous vous encourageons à rester pour une petite conclusion.

Je vais donner la parole à Olivier, ensuite à Pablo. Je ne sais pas si Pablo veut reprendre la parole. Ensuite, je vous encourage à envoyer vos questions sur la liste de diffusion.

Holly, allez-y.

HOLLY RAICHE : D'accord. S'il y a d'autres questions, nous y répondrons sur la liste de diffusion. Joanna, est-ce que vous pourriez mettre dans le chat le lien pour envoyer les questions ?

JOANNA KULESZA : Je vais le mettre dans le chat.

HOLLY RAICHE : Je vais donner alors la parole à Olivier. Olivier, allez-y, vous avez la parole.

OLIVIER CRÉPIN-LEBLOND : Merci Holly.

On a entendu quelque chose à propos d'un problème, la concentration de pouvoir. Il s'agissait d'une préoccupation et pour moi, cela donne lieu à moins de résilience, ce qui veut dire un problème de blackout, un problème de réseaux qui peuvent s'interrompre ou s'éteindre. Et certains fournisseurs de service cloud peuvent s'interrompre pour différentes raisons, par exemple un samedi soir. Est-ce qu'il y a des moyens de compenser cela à travers la notification de fournisseurs ?

Est-ce qu'on a trouvé un système qui nous permettrait de lutter contre ce manque de résilience ?

HOLLY RAICHE : Geoff, allez-y, vous avez la parole.

GEOFF HUSTON : Non. Je serai bref : non, cela n'existe pas.

HOLLY RAICHE : Merci Geoff.

Joanna, je pense que je vais vous donner la parole maintenant pour la conclusion et pour le quiz. D'abord, je veux remercier tout le monde d'avoir participé. Je veux remercier les membres d'APNIC. Et je donne maintenant la parole à Joanna.

JOANNA KULESZA : Merci beaucoup Geoff pour votre participation. Merci beaucoup à Holly également. Nous avons beaucoup apprécié d'entendre parler d'un point de vue gouvernemental. Et j'aimerais remercier les membres du GAC que nous avons vus sur la liste de participants. J'apprécie beaucoup de travailler avec le GAC et de bâtir nos collectivités communes.

Comment participer à ces webinaires ? J'ai reçu des courriels à ce sujet. J'aimerais donc que vous remplissiez tout d'abord ce petit questionnaire pour avoir un retour sur ce webinaire et sur les webinaires que nous pouvons toujours améliorer à l'avenir.

Gisella, est-il possible d'avoir ce questionnaire maintenant ?

GISELLA GRUBER : Oui. Est-ce que vous le voyez à l'écran ? J'espère que c'est possible.

JOANNA KULESZA : Non, il n'apparaît pas à l'écran.

GISELLA GRUBER : Est-ce que vous le voyez maintenant ?

JOANNA KULESZA : Non, je ne vois rien à l'écran. Voici le questionnaire, cela semble fonctionner maintenant.

GISELLA GRUBER : Très bien, excellent. Donc je vais vous lire les questions rapidement.

Première question : comment avez-vous entendu parler de ce webinaire ? Twitter, Facebook, la liste de diffusion At-Large, le calendrier At-Large, Skype, par un collègue ou autre. Je vous donne quelques secondes supplémentaires pour répondre à cette première question.

JUDITH HELLERSTEIN : Est-ce qu'on peut avoir plus d'une seule réponse ?

GISELLA GRUBER : Est-ce que vous avez essayé ? Je ne suis pas sûre que vous puissiez.

JOANNA KULESZA : Je ne pense pas qu'on puisse répondre avec plusieurs réponses, mais nous allons prendre note que ce serait un changement à apporter, de pouvoir donner plus d'une seule réponse. Indiquez la première manière dont vous avez entendu parler de ce webinaire, la première occurrence. Merci beaucoup.

GISELLA GRUBER : Un instant s'il vous plaît. Nous allons maintenant passer à la deuxième question. Désolée, petit problème technique pour passer à la question suivante.

JOANNA KULESZA : Gisella, je sais qu'il y a un autre webinaire dans deux semaines, donc je voulais vous en parler pour nous préparer à la prochaine réunion de l'ICANN. Nous sommes toujours à la première question sur l'écran. Il y a une question qui a réapparu à l'écran et c'est toujours la question 1.

GISELLA GRUBER : La question 2 semble être bloquée. Je suis désolée de ces problèmes techniques que nous rencontrons.

JOANNA KULESZA : Ce que vous pouvez faire peut-être, c'est d'essayer pour la prochaine fois de travailler à ces questionnaires. Est-ce que cela vous conviendrait ?

HOLLY RAICHE : Oui, tout à fait.

JOANNA KULESZA : Je vais donc conclure. Nous allons essayer d'obtenir votre retour par d'autres canaux.

Le prochain webinaire sera présenté par Jonathan Zuck. Nous allons bientôt avoir cette réunion de l'ICANN69 et nous voudrions vous inviter à nous parler de votre expérience virtuelle pour ces réunions et comment améliorer ces réunions virtuelles. Nous allons nous concentrer sur donner de meilleures présentations en ligne. Vous êtes tous invités pour ce webinaire pour cette nouvelle réalité que nous allons aborder lors de ce prochain webinaire à 13h00 UTC dans deux semaines. J'ai indiqué un lien ; vous pouvez avoir tous les détails grâce à cela pour cette réunion. Je pense que ce pourrait être une réunion très utile pour nous préparer.

Je vais conclure en remerciant nos invités. Holly, merci beaucoup. Merci également Geoff d'avoir répondu à ces questions tout à fait pratiques, merci pour vos observations. Merci à toutes et à tous de votre attention. J'apprécie beaucoup que plusieurs communautés nous rejoignent. Je remercie les personnes ayant préparé ce webinaire, le personnel. Merci également à nos interprètes, cela nous a permis de travailler entre plusieurs cultures et plusieurs langues.

Je vous souhaite une excellente soirée ou journée. On se retrouvera au prochain webinaire. Merci beaucoup.

GISELLA GRUBER : Merci à toutes et à tous. Le webinaire est maintenant terminé. Je vous souhaite une excellente journée ou fin de journée. Merci beaucoup. Au revoir.

[FIN DE LA TRANSCRIPTION]