MARRAKECH – Aspects politiques du DNS sur HTTPS (DoH), du DNS sur TLS (DoT) et questions connexes
Mardi 25 juin 2019 – 15h15 à 16h45 WET
ICANN65 | Marrakech, Maroc

ALEJANDRA REYNOSO : Bonjour à tous. Je vais vous demander de prendre place, nous allons commencer dans une minute. Merci beaucoup.

Est-ce que je pourrais avoir la présentation à l'écran s'il vous plaît ? Merci. Alors en attendant la présentation, merci à tous d'être avec nous. Nous allons avoir une séance de haut intérêt sur le DNS sur HTTPS et DNS sur TSL. Donc tout d'abord, l'ordre du jour sera que je vais d'abord vous présenter les objectifs de la séance, je vais vous présenter nos panelistes. Il y aura un aperçu général technique des sujets qui sera suivi par une partie questions et réponses. Ensuite, nous parlerons des préoccupations relatives au déploiement et ensuite, nous passerons aux questions et réponses. À la fin, nous aurons un panel, une discussion sur les considérations de déploiement. Donc nous espérons que tous vous participerez à ce sujet brûlant, sujet d'actualité.

Il y aura des micros dans la salle, donc vous vous manifesterez. Vous voyez, il y a différents nombres, quatre, six, trois et cinq là-bas à l'arrière de la salle. Ah, pardon, c'est là-bas. Donc lorsque

vous avez une question, levez la main aussi haut que possible de manière à ce que les micros puissent venir jusqu'à vous pour vous donner la parole.

Alors, on va préparer la présentation s'il vous plaît. Merci. Je vais commencer par me présenter. Je suis Alejandra Reynoso du ccTLD .gt, et je suis vice-présidente de la ccNSO. Et avec moi, j'ai Danny McPherson qui est vice-président exécutif et responsable de la sécurité à Verisign. Il est également membre du SSAC.

J'ai également avec moi Peter Koch qui travaille pour DENIC, le gestionnaire de ccTLD pour DE en tant que conseiller en politiques actuellement.

Et nous avons également avec nous Barry Leiba qui est responsable des normes à Futurewei Technologies. Barry a travaillé sur les technologies de courriels depuis la fin des années 1980 et il se concentre sur l'internet des objets, les plateformes de messagerie et autres, la sécurité, les droits privés sur internet, le développement des normes et le déploiement. Barry est également membre du SSAC.

Nous aurons Alyssa Moore qui est là-bas. Excusez-moi, je ne pointe pas du doigt les gens en principe. Mais elle est conseillère en politiques à CIRA qui est l'autorité qui est gestionnaire du CA.

Barry et Alyssa seront nos modérateurs pour la partie questions et réponses.

Et pour le reste des panelistes, nous avons Tim April. Tim April est architecte en sécurité chez Akamai Technologies, qui se concentre sur la sécurité du DNS et la réponse aux menaces, aux dangers. Et il est membre du SSAC également.

On va avancer un petit peu s'il vous plaît, diapositive suivante. Et nous aurons également Vittorio Bertola, qui est responsable des politiques et de l'innovation pour Open-Xchange, la société parente de PowerDNS. Et il travaille sur les conséquences de politiques sur le chiffrement du DNS dans différents domaines depuis quelques années déjà.

Et enfin, nous avons Michele Neylon, qui est fondateur et PDG de Blacknight Solutions, qui est un bureau d'enregistrement accrédité. Il est également membre du conseil de la GNSO.

Alors, avançons s'il vous plaît dans les diapositives. Nous avons apparemment des problèmes techniques, comme toujours. Mais ce n'est pas très grave. On va peut-être commencer la présentation technique générale sans les diapositives, je ne sais pas si c'est possible, simplement pour ne pas perdre de temps.

Alors, encore une petite minute pour voir si on peut afficher les diapositives sinon on démarre. Mais on va quand même leur

donner quelques secondes. Entre temps, vous pouvez toujours aller chercher les diapositives sur l'emploi du temps pour suivre la conversation mais je pense que maintenant, on va démarrer. Donc Danny, s'il vous plaît.

DANNY MCPHERSON : Très bien, je vais commencer sans les diapositives. Je crois que c'est déjà assez compliqué comme sujet sans les diapositives donc là, cela va être très intéressant.

Je suis Danny McPherson, je suis membre du SSAC et dans ce contexte, je présente ces diapositives au nom du SSAC. Donc l'erreur vient du SSAC, pas de moi. Non, je rigole.

Donc en ce qui concerne notre sujet, je vais parler du sujet technique et ensuite, Peter parlera des implications éventuelles. Mais le sujet général a généré beaucoup d'intérêt. Récemment, on parle de DoH et de DoT, donc DNS sur HTTPS et DNS sur TLS.

Et donc d'une manière générale, ces technologies ont pour objet la confidentialité des informations. Le DNS n'a pas de fonctionnalité de confidentialité et il n'y a pas non plus d'intégrité. Mais l'idée, c'est d'avoir les DNSSEC pour l'intégrité mais le DNS est toujours ouvert à tout ce qui est surveillance, gens qui écoutent ce qui se passe ou qui observent ce qui se passe pour différentes raisons. Cela peut aussi être un problème

de contrôle parental, de censure des États, de blocage à différents sites. Donc il y a différentes raisons pour lesquelles ceci est important. On vous expliquera un petit peu pourquoi par la suite.

Encore une fois, le cœur de la discussion, c'est que le DNS n'a pas vraiment de confidentialité en lui-même. Donc dans la géopolitique, dans le monde d'aujourd'hui, étant donné les conséquences économiques aujourd'hui, les transactions et la confidentialité, c'est quelque chose d'important.

Donc je vais parler des modèles de déploiement, pas vraiment de la politique. Mais si vous suivez, à la diapositive six, nous parlons de ce que je viens de dire. Donc sans la confidentialité des transactions du DNS, vous êtes ouverts à finalement que les gens puissent voir vos informations, comprendre où vous allez sur internet, miner ces informations. Donc la notion de DoH et de DoT, l'idée, c'est de fournir un chiffrement de ce qui se passe de manière à ce que s'il y a un observateur, un attaquant, cette personne ne verra pas les informations. Donc c'est vraiment à la base, ce dont on parle avec DoH et DoT.

Alors diapositive sept. Sur cette diapositive, vous avez la présentation générale du DNS traditionnel. Pensez un petit peu au DNS que vous avez. Vous avez donc un dispositif, vous avez une application sur votre dispositif et cette application souhaite

résoudre quelque chose dans le DNS et utilise un processus. Donc par exemple, vous allez demander à votre ordinateur comment je vais aller à www.exemple.com. Et votre dispositif a un résolveur DNS qui va parler à un réseau local ou à réseau du FSI.

On va avancer de deux diapositives pour arriver à la huit s'il vous plaît, donc la description du DNS traditionnel s'il vous plaît. Ah, il faut que je ralentisse, d'accord.

Alors, c'est ce que j'expliquais il y a un instant. Donc vous avez une application qui veut résoudre quelque chose pour l'utilisateur, un processus sur un diapositif. Donc l'application parle au système opérationnel traditionnel. Cela peut être par exemple une application sur votre iPhone, cela peut être un navigateur sur votre ordinateur. Donc cette application, ce navigateur va demander au système opérationnel local où est le nom de destination sur l'internet. Et ce dispositif va ensuite aller parler à un forwarder ou alors à un résolveur récursif. Alors en général, ce résolveur récursif fait partie d'un réseau local de FSI fournit par le local. Mais d'une manière générale, ils sont aussi dans le cloud. Cela peut être un DNS ouvert ou un serveur de noms qui existe dans le cloud. Donc c'est ce qui se passe au niveau de l'architecture. Parfois, les choses ne se passent pas au niveau local. Donc ce résolveur ensuite va vers celui qui fait

autorité, donc le premier niveau, cette infrastructure qui fait autorité, et résout le nom, le fait passer à l'application ou au résolveur minimum qui ensuite le redonne à l'application qui ensuite peut se connecter à la destination sur l'internet qui est donc recherché.

Comme vous le voyez dans ce diagramme, toutes ces transactions, il n'y a pas de confidentialité des transactions. S'il y a un observateur qui observe le cheminement, en vert sur les flèches, cette personne peut savoir ce que souhaite faire la personne. Il peut y avoir des problèmes de concurrence, ce peut être un problème de sécurité, un contenu sensible, etc. Donc l'idée, c'est de protéger ces informations.

Alors, passons à la diapositive suivante. Une des deux solutions, c'est donc le DoT, le DNS sur TLS. Donc TLS, c'est la sécurité de couche de transport. Donc les transactions sécurisées sur l'internet, en général si vous voyez le petit verrou, par exemple si vous allez sur un site financier ou d'informations confidentielles, en général on utilise le TLS. Donc c'est un chiffrement TLS pour protéger la confidentialité des informations. Donc s'il y a une attaque en chemin, les informations ne peuvent pas être manipulées ou volées.

Dans le modèle DoT, diapositive suivante, ce qui se passe dans ce modèle... Le DoT peut être déployé par différentes

techniques. Il y a différentes normes sur lesquelles on travaille dans la communauté. Mais le DNS sur TLS en général prévoit qu'un système local, par exemple votre iPhone ou votre laptop, peut avoir un système général qui dit : « Je vais utiliser ce résolveur dans l'infrastructure pour résoudre quelque chose, tout ce que j'ai sur le DNS. » Donc les applications utiliseront ces paramètres pour se rendre où on veut aller. Donc un navigateur fera la même chose, il va demander au résolveur minimum : « J'ai besoin d'aller sur exemple.com sur internet. Est-ce que vous pouvez résoudre ceci ? »

Alors ce résolveur minimum passe par une chaîne chiffrée et il va aller soit dans le cloud, soit dans le réseau FSI. Ce que vous voyez sur ces flèches rouges, de cette manière, personne ne peut manipuler, avoir accès à ces informations qui sont sur ces flèches rouges et voir ce qui se passe.

Et ensuite, dans l'infrastructure, quand on passe au serveur qui fait autorité, on ne sait pas exactement comment intégrer le DoH ou le DoT à la racine, au TLD ou sur une infrastructure de deuxième niveau, donc on est toujours en train de travailler à ceci.

Et nous allons mettre ceci en contraste avec le DoH, qui en fait déplace un petit peu en arrière le chiffrement. Parlons maintenant du DoH. Je vais trop vite, d'accord.

Donc à la base, plutôt que d'utiliser TLS pour le transport, le DoH se dit : « Alors, j'ai beaucoup d'applications sur mon dispositif, j'ai beaucoup de trafic sur le web, j'ai beaucoup de logiciels par rapport à des transactions HTTP qui opèrent sur ce dispositif. Donc plutôt que d'utiliser le TLS dans l'infrastructure, je vais coder les réponses, les requêtes en requêtes HTTP. Et ensuite, je vais le mettre sur TLS – c'est justement comme cela que ça fonctionne – et je vais les transférer dans le réseau. Donc cela donne beaucoup de crochet en fait pour l'application puisqu'elle peut entrer en transaction avec l'infrastructure directement et en fait complètement contourner le résolveur minimum. Je vais vous montrer à quoi cela ressemble sur la diapositive suivante.

Voilà un modèle de déploiement qui peut être différent. Mais mon navigateur peut utiliser un nom de serveur résolveur de l'infrastructure, une autre application pourra utiliser quelque chose de local ou celui de mon système.

Ce qui est intéressant, là, c'est que si quelque chose se casse dans ce scénario, notre application qui utilise le DNS, c'est un petit peu complexe à comprendre mais ce qui se passe, c'est que les FSI traditionnellement utilisent les requêtes DNS comme point de contrôle dans l'infrastructure ou alors une entreprise pourra faire la même chose. Donc ils ne veulent pas que les

transactions chiffrées aillent directement aux applications parce qu'on perd une certaine visibilité, une certaine sécurité, les contrôles parentaux, etc.

Donc le cœur de cette notion, c'est que plutôt que d'utiliser le résolveur minimum, l'application va envoyer sa requête à l'infrastructure internet, l'infrastructure de résolution, et donc va contourner tout ce qui existe dans le système opérationnel et même au niveau du réseau local. Et c'est ce que montre cette diapositive.

Donc, une autre chose qui est intéressante et que j'aimerais vous expliquer, c'est que si vous regardez ceci du point de vue de la surveillance, du point de vue de l'écoute, le DoH en fait mélange le trafic de résolution DNS avec d'autres trafics HTTP sur le réseau. Donc il est beaucoup plus difficile de faire de la surveillance, d'observer ce qui se passe, de filtrer parce qu'en fait, il faut comprendre tout le trafic, il faut trouver des failles dans tout le trafic avec les requêtes de résolution DoH. DoT encore une fois, c'est un système qui est beaucoup plus global.

Et dernière chose que je souhaite dire par rapport à cela, les modèles de déploiement que vous voyez pour DoH et DoT ici peuvent être mélangés ou alors on peut inverser les différents domaines. Cela dépend un petit peu de ce que l'on veut activer

au niveau de l'application ou autre. Donc un système minimum pourra utiliser DoH ou DoT ou le DNS traditionnel.

On n'a pas trop réfléchi à tout ce qui fait autorité, le routcom, .edu, etc. Donc c'est surtout au deuxième niveau. Il y a d'autres techniques comme le QName qui protège un petit peu la vie privée mais il y a différents aspects qui présentent des problèmes.

J'ai vraiment parlé très très vite. J'espère que j'ai rattrapé le retard. Mais nous allons faire une pause pour voir si vous avez des questions là-dessus avant de passer à Peter et à sa présentation sur le déploiement. Donc si vous avez des questions, peut-être que vous pouvez les poser maintenant ou alors vous pouvez laisser parler Peter et poser vos questions plus tard. Peter va parler des implications de DoH et DoT.

ALEJANDRA REYNOSO : Merci Danny pour cette excellente explication très rapide. Nous avons une question ici. Merci beaucoup.

NIGEL CASSIMIRE : Nigel Cassimire, je viens de l'Union caribéenne des télécommunications, la CTU.

Bonjour, c'est complètement nouveau, j'essaie de comprendre le problème que vous cherchez à résoudre ici. Est-ce que vous cherchez à rendre le DNS plus sécurisé ? Et en quoi est-ce que cette technique peut être comparée avec le DNSSEC par exemple ?

MICHELE NEYLON : Alors nous sommes en train de nous battre pour savoir qui va parler, donc je vais prendre le micro.

Les DNSSEC sont souvent quelque chose dont on parle dans les milieux de l'ICANN comme si c'était en fait la baguette magique pour résoudre tous les problèmes de DNS. Ce n'est pas le cas. Les DNSSEC sont un moyen, par exemple lorsqu'on va à bank.jenesaisquoi, de s'assurer que vous allez bien dans votre banque, de manière à ce que personne ne s'insère au milieu.

Donc il s'agit d'empoisonnement, ce qui a été un problème par le passé. Donc nous avons pu avec le DNSSEC résoudre ceci. Avec le DoT et le DoH, cela ajoute un certain niveau de la protection de la vie privée, mais il y a des problèmes avec les deux en fait. La vie privée et la sécurité. Mais effectivement, il y a un impact entre l'un et l'autre, entre la protection de la vie privée et la confidentialité. Mais c'est la manière dont les recherches sont faites par les dispositifs, que ce soit votre

dispositif mobile, votre iPad, votre ordinateur, c'est en fait déplacer ces requêtes du DNS traditionnel pour se rattacher à d'autres protocoles. Donc dans le cas du DoH, c'est en fait des requêtes web.

Alors ne je suis pas aussi bon en technique que lui, il pourra me corriger, mais c'est en fait l'approche simple.

ALEJANDRA REYNOSO : Merci Michele.

Nous avons d'autres participants.

ARIEL LIANG : Il y a deux participants à distance. Mohamed Yousif : « Est-ce que DNS sur TLS cause des dégradations en matière de performance en termes de délais de résolution d'une requête ? »

Et je lirai la prochaine question par la suite.

MICHELE NEYLON : Cela dépend de la manière dont le résolveur minimum est mis en œuvre. Donc il y a le temps de connexion initial mais si cette connexion persiste dans le temps, s'il est prévu pour faire cela, le temps de résolution est le même en principe que pour le DNS.

ARIEL LIANG : Deuxième question d'un participant à distance, de Yazid Akanho du Bénin : « Diapositive six, les technologies telles que la minimisation QName peuvent être aussi efficaces pour protéger la vie privée. Que peut-on dire là-dessus ? »

DANNY MCPHERSON : On ne voulait pas trop parler de la minimisation QName mais c'est une technique assez légère. Traditionnellement, si je souhaite résoudre quelque chose avec le DNS, je dois avoir un nom de domaine entièrement qualifié. Donc les serveurs tel que, je ne sais pas, internalsecreteserver.info.verisign.com, donc je dois ajouter cette question sur tout le chemin mais en fait, la racine avait seulement besoin de me dire l'étape suivante dans le .com, dans la hiérarchie. Donc je n'avais pas besoin de tout demander, je dois simplement savoir comment aller vers le .com. Et une fois que je le sais, je peux arriver à mes serveurs internes secrets. Donc pas besoin de divulguer tout le serveur. Donc de cette manière, on peut minimiser. C'est une fonction qui permet de minimiser le travail. C'est une fonction qui est déjà prête dans toutes les mises en œuvre de serveur minimum mais cela minimise les attaques du point de vue de la protection de la vie privée.

ALEJANDRA REYNOSO : Merci beaucoup. Je vais demander à tout le monde de se concentrer sur le sujet et de ne pas poser des questions trop larges sur la sécurité et sur l'internet. Nous nous concentrons vraiment sur DoT et DoH. L'idée, c'est vraiment de permettre au panel de se concentrer sur le sujet. Il y a une question aux micros quatre et ensuite cinq et ensuite, nous passerons à l'intervenant suivante.

FRED BAKER : J'ai été un petit peu surpris par votre réponse par rapport à la différence entre TLS et les DNSSEC parce qu'en fait, ils sécurisent des choses qui sont différentes. Le DNSSEC sécurise le contenu, l'enregistrement de ressources alors que le TLS sécurise le canal.

C'est un petit peu comme les tuyaux et l'eau. Si j'ai un tuyau qui est magnifique, très solide, le meilleur tuyau du monde et qu'en amont, j'ai un lac que j'ai rempli de poison, lorsque l'eau arrive dans ce magnifique tuyau, l'eau qui arrive en fait est toujours empoisonnée.

Donc sécuriser le contenu permet de se débarrasser du problème de poison. Donc avoir un bon tuyau, un bon canal, c'est une bonne chose, certes, mais les DNSSEC sont quand

même très importants pour s'assurer que le nom transporte bien ce que l'on veut.

DANNY MCPHERSON : Oui, effectivement, vous avez tout à fait raison, Fred. Même si on ajoute DoH ou DoT entièrement déployé dans l'écosystème, il faut quand même avoir les DNSSEC et la minimisation QName pour vraiment bien protéger parce qu'en fait, ils s'occupent de différentes choses.

ALEJANDRA REYNOSO : Merci.

Numéro cinq.

JIM PRENDERGAST : Je ne suis pas membre de l'IETF. Je sais qu'il y a beaucoup de personnes qui sont à l'IETF.

Vous avez parlé des avantages, Danny, et également de ce qui peut se briser ou être défaillant. Comment approuver une norme si certaines de ces choses se passent et qu'il y a en fait des conséquences auxquelles on ne s'attendait pas ?

ORATEUR NON-IDENTIFIÉ : Oui, votre question est tout à fait justifiée.

DANNY MCPHERSON : Je crois que la technologie existe, l'écosystème s'adaptera pour en fait trouver quel est le bon modèle de déploiement. Personne dans l'écosystème, que ce soient les navigateurs, que ce soient les opérateur de serveurs quels qu'ils soient, ne souhaite qu'il y ait des défaillances.

Maintenant, certes, il y a des problèmes de déploiement. Si vous êtes un FSI et que vous n'avez pas de visibilité par rapport aux utilisateurs et que ces personnes qui utilisent leur navigateur utilisent le cloud et qu'ils vous demandent de résoudre un problème de DNS, vous ne pourrez peut-être pas le faire. Ou alors si vous souhaitez avoir des contrôles parentaux, et bien il est possible que vous ne puissiez pas le faire. Alors il faudra que le système soit ajusté. Et c'est important avec DoH et DoT de se rendre compte que les modèles de déploiement vont varier, vont être adaptés au fil du temps avec les variations sur le marché et au fur et à mesure qu'on détermine ce qui fonctionne et ce qui ne fonctionne pas.

ALEJANDRA REYNOSO : Merci beaucoup.

Donc pour résumer, nous allons maintenant parler dans préoccupations éventuelles relatives au déploiement.

PETER KOCH : Merci Alejandra. Je m'appelle Peter Koch. Je suis conseiller principal et un des délégués ccNSO co-conspirateurs de ce groupe de travail.

J'ai été invité à parler des problématiques ou problèmes qui pourraient se poser avec le déploiement de ce type de système. Le protocole est innocent et des choses se passent. Et c'est probablement ce qui va poser certaines difficultés.

La première partie était technique. Nous avons donc deux normes qui s'occupent à peu près...

ALEJANDRA REYNOSO : Excusez-moi, est-ce qu'on pourrait montrer à la diapositive suivante ? Très bien.

PETER KOCH : Très bien. Alors, nous avons deux normes qui de manière légèrement différentes s'occupent de la même chose, à savoir la confidentialité des données. Et je rappelle aux gens pourquoi on pense à cela.

Il y a eu l'affaire Snowden il y a quelques années où l'on a découvert que le trafic DNS peut être une source d'informations, de renseignements et peut être utilisé pour identifier des gens, identifier des actions que font les gens sur le web.

Maintenant, on va se focaliser sur le DNS, mais il y a d'autres services. Il y a des documents qui ont été publiés au sein de l'IETF qui parlent de cette surveillance qui doit être faite par rapport aux menaces que représente l'internet. Donc la réponse pour cette surveillance, c'est le chiffrement. Donc ici, on parle de chiffrement des informations qui sont transportées sur internet.

Et je veux ajouter que ce n'est pas seulement pour les acteurs qui l'utilisent mais aussi pour d'autres parties de ce puzzle qui peuvent avoir un intérêt à utiliser ces informations, parce que l'information sur le DNS est libre et donc le fait que l'on puisse l'interroger, cela représente des informations très valides et très intéressantes.

On décrit comment d'une partie le résolveur communique avec une autre partie. Dans ce cas, on l'appelle le DoH. Alors de l'extérieur, on pense que c'est un serveur mais il y a une réponse DNS. Ce que l'on n'a pas résolu jusqu'à maintenant, c'est comment le navigateur dans ce cas obtient les informations, à qui adresser la requête. En général, c'est le système d'exploitation qui donne ces informations ; c'est le cas pour la

plupart des ordinateurs portables et des téléphones. La résolution de noms est enterrée dans le système d'exploitation. Et cela a été utilisé dans les dispositifs que vous avez sous les yeux en général.

Mais cela pourrait changer. L'idée pour les développeurs, c'est de travailler à des configurations automatiques pour trouver ces informations. Il y a également des initiatives en cours pour donner aux utilisateurs plus de choix pour qu'ils puissent configurer de manière manuelle le DNS. Mais cela est encore en cour d'évaluation.

Il y a eu un navigateur, un fournisseur de navigateurs qui a activé DNS sur HTTP, DoH, et cela contient un URL codé en dur qui est identifié sur l'adresse web que vous voyez quand vous visitez une page web. Donc cette information est codée en dur. Toutes les informations sont là à un moment donné et on utilise un résolveur particulier DoH. Et cela va remplacer l'information qui est codée en dur et qui est donnée par le système d'exploitation. Donc l'application va savoir qui doit utiliser un autre acheminement de résolution différent de celui qu'utilise le système d'exploitation.

Cela pose certaines difficultés, bien sûr, car cela peut interférer avec certains gestionnaires de réseau et certaines politiques des gestionnaires de sécurité qui essaient de gérer l'information

différemment en interceptant ce trafic, comme quelqu'un l'a déjà évoqué.

Alors, la question intéressante est de savoir pourquoi il y a deux normes. J'essaie de ne pas rentrer dans les détails techniques mais DoT, c'est-à-dire DNS sur HTTP sur la couche de transport, c'est un truc qui a plus à trait avec l'ingénierie parce qu'il y a plusieurs couches. Mais il a un problème, à savoir qu'il y a certaines informations dont vous avez besoin qui doivent passer le pare-feu pour pouvoir être obtenues.

Le trafic DoH, c'est comme l'accès à un site web ; cela a l'apparence comme si vous accédez à un site web. Alors n'importe qui ne peut pas bloquer l'accès à ce service de résolution DoH sans en même temps bloquer l'accès à des serveurs web importants. C'est le problème. Et il y a des recherches en cours pour ajouter cette configuration à cette approche du DNS sur HTTP, DoH. Côté technique, il y a d'autres détails que je ne vais pas citer aujourd'hui.

Donc on ne pourrait pas bloquer des résolutions de noms parce qu'en même temps, cela bloquerait l'accès à des sites web ou à des moteurs de recherche populaires. Cela pourrait ou non interférer avec certaines exigences au niveau de la réglementation où les FSI doivent bloquer certaines résolutions de noms de domaine. Et quand je dis cela, je ne dis pas que ces

mécanismes de blocages sont efficaces mais qu'ils peuvent être des conditions réglementaires dans certains pays. Ceci dit, cela n'a jamais été parfait parce qu'on peut les contourner en utilisant un VPN ou en faisant marcher votre propre résolveur.

Masquer les requêtes DNS dans le trafic peut aider les utilisateurs à contourner ce type de censure lorsqu'il y a un filtrage des informations ou bien cela peut bloquer les logiciels malveillants lorsqu'un utilisateur souscrit à un site web. Diapositive suivante s'il vous plaît.

Alors, voilà un petit peu quelle est la situation générale. DNS sur HTTP ne prescrit pas un modèle de déploiement en particulier. Toute entreprise peut faire fonctionner un résolveur DNS qui pourrait pointe vers un navigateur. Mais nous pouvons constater d'ores et déjà un certain modèle de déploiement qui va vers une certaine concentration ou consolidation. Et donc les fabricants ou les fournisseurs de navigateurs et les fournisseurs de solutions DNS pointent les utilisateurs vers les services de résolution d'un fournisseur en particulier, ce qui donne beaucoup d'informations au fournisseur et ce qui contribue aussi à la stabilité. Mais cela pose le problème de la concentration.

Au cours des 30 dernières années, le système était assez décentralisé au niveau des FSI ou au niveau de vos ordinateurs,

de vos dispositifs. Or, la résolution DNS a évolué et au fil du temps, il y a ce qu'on appelle les quads comme 1.1.1.1. Il y a des pays où des gens doivent faire face à des blocages de certains sites web. Et il y a d'autres systèmes qui utilisent ce même type de démarche.

Mais ces aspects, en plus du choix d'acheminement de résolution par le FSI ou par l'utilisateur, cela conduit à une concentration de plus en plus importante de résolveurs qui devient de plus en plus grande, de plus en plus importante. C'est-à-dire que la population de ces résolveurs ne fait que s'accroître, donc les politiques liées à cette concentration deviennent de plus en plus importantes.

Alors comme on l'a dit, DoH et DoT fournissent des systèmes de confidentialité ou de protection de données. Que ce soit les résolveurs du FSI ou les résolveurs qui sont fournis par les services de résolution DNS, ils voient les requêtes des utilisateurs avec différents niveaux de détails. Pour certaines raisons, parfois il y a des informations qui sont ajoutées aux requêtes pour que les utilisateurs obtiennent des réponses sur mesure. Certains scénarios techniques dépendent du fait que tout le monde n'obtient pas les mêmes réponses lorsqu'on interroge les serveurs de la même manière Et le DNS est souvent

utilisé pour diriger les utilisateurs vers les systèmes de contenu qui puissent réduire un maximum de latence.

La confidentialité n'a pas seulement trait au chiffrement mais aussi aux politiques DNS car les opérateurs peuvent vous promettre qu'ils seront responsables de ce qui se passe au niveau des interrogations au résolveur, que ce soit au niveau du FSI ou des gens qui peuvent être intéressés à vos données. Diapositive suivante s'il vous plaît. Il y a une diapositive encore, s'il vous plaît. Ça n'a pas marché... Très bien.

Alors pour ce qui est des politiques concernant les résolveurs DNS, comment doivent-ils être sélectionnés ? Nous avons vu quels sont les moyens techniques, comment les utilisateurs décident quel résolveur utiliser et comment ils le configurent dans leur application et comment les opérateur des ces résolveurs DNS sont responsables de ce qu'ils promettent et de ce qu'ils font parce qu'une fois de plus, ils doivent parfois diffuser des informations à la demande de certaines entités, comme par exemple les forces de l'ordre.

Et qui détermine quelles sont les politiques acceptables ? Cela, c'est une autre discussion. Il y a des fournisseurs qui disent : « Oui, on comprend qu'il y a des débats dans la communauté et nous sommes prêts à agir autrement. Mais nous aimerions avoir certaines politiques en matière de résolveurs qui

nous disent ce qu'il faut faire ou ne pas faire par rapport à certaines requêtes. »

Panorama général parce que l'une des questions, c'est de dire pourquoi parle-ton de ceci dans le contexte de l'ICANN. Il y a un groupe de fournisseurs de solution DoH DoT qui pensent qu'il y a une certaine implication, un service qui est utilisé sur internet comme le web comme nous le faisons tous. Et parfois, il est intéressant d'explorer une piste pour essayer de trouver d'autres moyens de résolution. Comme par exemple le .onion qui peut être utilisé pour certaines requêtes.

Pour parler de manière pratique, quand nous avons ce groupe de fournisseurs de solution de résolution, il y a une grande population qui voudrait être dans la position de décider d'ouvrir ou non de nouveaux segments de l'espace de noms de domaine. Et qu'est-ce que cela impliquerait pour le rôle de l'ICANN en tant que coordinateur de la zone racine s'il y a une modification au niveau du pouvoir, si les gens par exemple votent à travers leur navigateur ?

Conclusions, conclusions préliminaires probablement. Nous avons appris que certains déploiements de DoH DoT peuvent avoir un impact sur les points de contrôle traditionnels au niveau de la résolution. FSI, entreprises peuvent intercepter les requêtes et envoyer des réponses différentes pour par exemple

faire de la publicité mais aussi pour délier des utilisations malveillantes.

Les résolveurs, comment les sélectionner ? Cela est en cours de discussion. Pour les opérateurs de registre et les bureaux d'enregistrement actuellement, il y a un impact minimum. Or, il pourrait y avoir quelqu'un qui regarde la porte des bureaux d'enregistrement et des registres et dit : « Pourquoi vous ne voulez-pas me donner une copie de toutes les données DNS pour que l'on puisse répondre à vos utilisateurs de manière beaucoup plus rapide ? »

Et quel sera aussi l'impact sur les usagers ? Et cela est lié aussi aux DNSSEC est à la minimisation QName. Très bien, diapositive suivante.

ALEJANDRA REYNOSO : Merci beaucoup Peter. Y a-t-il des questions du public ? Nous avons le temps de répondre à quelques questions. J'ai numéro cinq.

WARREN KUMARI : Bonjour, Warren Kumari. Je travaille pour Google.

Peter, dans votre présentation, vous avez parlé d'un modèle de déploiement, celui des navigateurs. Cela n'est pas le modèle

.onion et donc on veut permettre aux usagers d'agir de manière différente.

Par exemple si on peut utiliser DoH, ils peuvent le faire, soit en utilisant les résolveurs du FSI ou en utilisant la solution DoH. Ils peuvent le faire.

Mais si les usagers veulent, ils peuvent choisir un autre résolveur et c'est un petit peu ce qui se passe actuellement où on a les résolveurs FSI mais on peut en choisir un autre.

Or, cela ne va pas changer ce que choisissent les usagers et nous ne demandons pas aux utilisateurs d'utiliser les services Google. Les protections existantes qu'ont les gens par rapport aux logiciels malveillants, tout cela continuera à marche de la même manière. La manière dont cela est déployé, c'est ce qui importe et non pas vraiment ce qu'est le transport en lui-même.

Est-ce que vous avez des commentaires par rapport à cela ?

PETER KOCH : Oui. Nous n'avons pas mis de nom sur la diapositive et j'espère ne pas avoir cité de nom. Merci de l'avoir fait parce que pour ce cas en particulier, c'est un ajout important au scénario du modèle de déploiement qui n'a pas été exhaustif dans ma

présentation. Les différents modèles sont en cours de discussions et celui dont vous avez parlé fait partie de cette liste.

Pour l'autre partie, j'aimerais me remettre à une discussion qui aura lieu ultérieurement. Je vais me focaliser sur les questions plus directes par rapport à ma présentation.

ALEJANDRA REYNOSO : Nous avons un participant à distance et puis nous allons continuer.

ARIEL LIANG : Il y a une question de Dirk Jumpertz : « On peut utiliser le DNS pour insérer les vecteurs data sur les enregistrements DNS. Connaissez-vous cela ? C'est très difficile à bloquer parce que les utilisateurs utilisent un canal fiable pour attaquer. HTTPS combiné avec DNS, est-ce que cela ne complique pas les choses ? »

PETER KOCH : C'est une information intéressante. Je n'étais pas au courant de cela. Peut-être que le reste des membres du panel souhaiteraient en parler plus tard.

ALEJANDRA REYNOSO : Numéro trois.

EDUARDO DIAZ : Eduard Diaz, président de NARALO. J'ai une question. Un problème potentiel pour l'usager est que si je télécharge par exemple une application et que cette application utilise son propre résolveur sans que je le sache, cela peut affecter un utilisateur qui n'est pas au courant de ce qui se passe en coulisses.

PETER KOCH : Merci de cette remarque. Un aspect dont on n'a pas parlé, c'est qu'en théorie, différentes applications pourraient donner différents résultats. Donc le système DNS pourrait avoir une apparence différente en fonction qu'il s'agisse du téléphone, de l'ordinateur ou du navigateur. Parce qu'en fonction de ce que vous utilisez, certains éléments pourraient bloquer. Cela, oui effectivement, pourrait poser problème à l'usager. Mais c'est le tout début de ce type de solution.

ALEJANDRA REYNOSO : Numéro quatre.

REMMY NWEKE : Je m'appelle Remmy Nweke. Je viens du Nigeria. Je représente la NCUC. Ma question concerne un des points de la diapositive lorsqu'on parle de l'impact de DoH et DoT sur les usagers. Nous pouvons essayer de voir quels seraient les impacts négatifs sur les usagers.

J'aimerais aussi obtenir des clarifications par rapport aux contre-mesures que nous pourrions utiliser pour atténuer ces impacts négatifs du DoH et DoT. Et aussi, quelles sont les responsabilités des usagers ? Quelles sont les implications au niveau des coûts, non seulement au niveau technique, au niveau des usagers ?

PETER KOCH : Je crois que c'est une contribution et pas vraiment une question mais qui peut quand même alimenter la discussion.

Nous avons encore deux diapositives avant de passer la parole au panel. Je ne vois plus de question.

ALEJANDRA REYNOSO : Non, nous allons donc passer directement au panel. Donc on va avancer un petit peu. Voilà, merci beaucoup. Donc les panelistes vont répondre à ces questions que vous voyez devant vous. Je vais les lire à haute voix.

Est-ce que vous prévoyez un impact du déploiement du DoH et/ou du DoT sur vos opérations ?

Y a-t-il des problèmes relatifs au DoH/DoT qui tombent dans le cadre de la mission de l'ICANN ?

Comment pensez-vous que le DoH doit être mis en œuvre dans des applications tels que les navigateurs web ?

Quelles sont vos préoccupations par rapport au DoH et/ou DoT ?

Donc nous allons commencer par Tim.

TIM APRIL : S'il fallait que je réponde à toutes les questions, cela prendrait très longtemps. Mais étant donné que je travaille dans la sécurité, celle qui me préoccupe le plus, c'est « Quelles sont les préoccupations par rapport au DoH et au DoH ? » C'est surtout l'usager final, quelle est leur perception de l'espace des noms. Celle-ci pourrait évoluer.

Du navigateur, de l'application au résolveur, si cette première partie utilise le DoH ou le DoT, vous avez une protection pour la vie privée. Mais vous ne savez pas que ceci ira jusqu'au serveur qui fait autorité. Vous n'avez pas de protection à ce niveau-là.

Donc si ce qui vous préoccupe c'est la fuite de données dans la communication, cela se passera au-delà du résolveur et parfois, cela pourra en fait revenir comme impact sur l'usager final.

Donc suivant l'implémentation ou la mise en œuvre, surtout avec le DoH, si votre application utilise un résolveur DoH sans que vous ne le sachiez, vous vous direz : « Il y a un problème de résolution au niveau du résolveur du FSI qui ne saura pas ce qui s'est passé. » Donc vous aurez un problème continu. Cela aura un impact sur l'usager final. Mais s'ils ne connaissent pas bien la technologie, ils ne sauront pas quoi faire.

Voilà, c'est tout ce que je vais dire. Je ne vais pas m'étendre davantage.

ALEJANDRA REYNOSO : Vittorio peut-être ?

VITTORIO BERTOLA : Alors, j'ai plusieurs choses à dire.

Par rapport à la première question, pour les plus grands FSI, nous avons un impact pour la mise en œuvre du protocole pour qu'il fonctionne dans le monde réel. Mais ce n'est pas le vrai problème. Ce qui nous préoccupe, c'est les sociétés open source

et de logiciels par rapport à l'impact que cela pourra avoir par rapport à la forme du DNS et du marché en général.

Je crois que la vraie problématique, ce n'est pas le chiffrement, ce n'est pas le transit, la connexion – c'est très bien pour la protection de la vie privée –, mais c'est l'ajout au DNS, le changement d'un service de réseau qui existe dans votre système opérationnel comme le TCP IP qui est quelque chose qui est géré par chaque application.

Et ceci présente un certain nombre de problèmes qui en partie veut dire que certaines applications choisiront différentes choses, c'est une chose. Mais ce qui est vraiment préoccupant, c'est que le marché des applications, surtout dans le web qui est en fait l'application la plus utilisée, tout ceci est beaucoup plus concentré. Donc si vous voulez mettre 95 % des requêtes DNS, vous devez utiliser les premiers DNS. Et tout fait partie de la même juridiction et du même pays.

Donc en termes de potentiel en politiques, en termes de juridiction et de souveraineté, toutes ces questions, cela change beaucoup de choses. Nous savons tous que pour les gouvernements, il y a encore plusieurs unités constitutives qui sont affectées, les FSI certes, mais dans ce contexte, nous parlons des gouvernements et des usagers.

Donc l'impact, la question pour les gouvernements, c'est vraiment la perte de contrôle pour la résolution du DNS. Donc il faudra considérer les contrôles parentaux, le filtre aussi des citoyens. Tout ceci, c'est une perte de contrôle. Donc les navigateurs web, ceux-ci modifient en fait la manière dont les contrôles sont gérés. Voilà pourquoi il faut prêter attention à ceci et je pense que les gouvernements vont le faire.

Et pour les usagers, il y a le problème du choix parce que si l'application décide d'envoyer une requête DNS à je ne sais qui... Même le fait de limiter les choix. Nous sommes les personnes qui décident qui peut utiliser les résolveurs, donc nous permettons ces utilisations. C'est à deux de décider des politiques. Donc en fin de compte, cela dépendra des politiques.

Et mon dernier message, c'est que cela dépend du modèle de déploiement. Mais se mettre d'accord sur le modèle de déploiement nécessitera des politiques mises en place de manière ascendante de manière à ce que les gens des applications ne fassent pas ce qu'ils veulent librement.

ALEJANDRA REYNOSO : Merci Vittorio.

Michele ?

MICHELE NEYLON : Je crois que les questions que nous sommes en train de considérer ne sont pas simples. Ce sont les questions difficiles, celles que l'on aime. Et je crois que certaines des questions sont assez théoriques et académiques. Et je pense qu'on en est au tout début du DoH et du DoT. Jusqu'à récemment, ceci était hypothétique et maintenant, cela devient réalité.

Donc quel va être l'impact sur la réalité ? Par exemple, la deuxième question. La mission de l'ICANN pourrait souffrir d'un impact par rapport à tout ceci. Par exemple, les identificateurs publics pourraient ne plus être publics et on se retrouverait dans une situation où on a beaucoup moins d'opérateurs de résolveur de DNS. Et alors il faudra déterminer ce qui est sur le DNS, ce que les gens peuvent obtenir, ce à quoi ils peuvent accéder. Donc c'est une conséquence potentielle.

Ma société est un bureau d'enregistrement. Nous avons également un service FSI. Et en fait, les gens ne comprennent pas ce qu'est un nom de domaine, ils ne comprennent pas la différence entre un nom de domaine et un navigateur. Ils ne comprennent pas la différence entre un moteur de recherche et la barre d'adresse d'un navigateur.

Donc lorsque quelqu'un dit : « Oui, l'usager peut choisir de changer le service qu'il utilise. », c'est peut-être vrai si vous parlez à un groupe de geeks qui sont à fond dans tout cela. Mais combien de personnes dans cette salle ont leur propre serveur de noms ? Bien. Je vois bien que vous êtes les geek donc, les geeks passionnés. Combien d'entre vous avez vos propres serveurs de courriels ? Et en plus, c'est les mêmes ! Alors honnêtement, est-ce que vous pourriez dire que vous êtes l'usager moyen ? C'est cela le problème, parce que dire qu'il y a un choix, ce n'est pas complètement vrai. Et en fin de compte, le type de politiques, le type d'aspects techniques dont on parle, c'est vraiment ce qui ouvre la boîte de Pandore.

Si on revient à la présentation de Danny et si vous regardez la comparaison entre les différentes technologies, la question à se poser, c'est pourquoi est-ce qu'on en est là ? D'où est-ce que cela sort ? Et la réalité, c'est que dans le monde dans lequel nous sommes actuellement, les questions de sécurité et de protection de la vie privé sont vraiment des questions qui préoccupent les gens. Si cela ne vous préoccupe pas, où étiez-vous ces dernières années ?

Donc il y a eu un certain nombre de questions intéressantes dont on a parlé. Donc maintenant, nous avons les moyens éventuels de pouvoir réparer ces problèmes que nous avons

découverts. Mais ceci nous fait découvrir d'autres problèmes, donc cela veut dire que nous serons tous employés pendant le reste de notre vie en gros.

Et du point de vue opérationnel, je ne sais pas exactement comment je vais expliquer à certains de mes clients pourquoi certaines choses ne fonctionnent pas. C'est déjà suffisamment problématique lorsqu'ils vous téléphonent et qu'ils vous disent : « J'ai des problèmes avec Outlook. » alors qu'en fait, ils n'utilisent même pas Outlook. Ils pensent qu'Outlook est leur client courriel.

Donc je crois quia des questions opérationnelles intéressantes dont il va falloir s'occuper.

Si vous regardez ce qui va se passer au cours des mois à venir, au fur et à mesure que ceci est lancé sur un certain nombre de navigateurs, un petit nombre de navigateurs, sur certaines applications, vous aurez des préoccupations en matière de sécurité. Vous aurez des gens qui vont trouver de nouvelles manières d'exploiter la technologie, les enregistrements TXT pour répandre un programme malveillant. Les gens vont se dire : « Cela fait peut. Pourquoi n'y ais-je pas pensé ? » Ce n'est pas une blague. En fait je ne sais pas, c'est peut-être une blague.

Mais il va falloir vraiment considérer les choses de près. Personnellement, j'ai beaucoup de préoccupations par rapport à l'idée de donner ce contrôle, cette décision à quelqu'un d'autre. Et je me dis : « Est-ce que je vais pouvoir moi-même dans mon bureau protéger mon personnel des programmes malveillants et des attaques ? Est-ce que j'ai la technologie pour le faire ? » Et je pense que la réponse, c'est non. Est-ce que c'est mauvais fondamentalement ? Pas nécessairement, non. Mais il va falloir que cela évolue.

ALEJANDRA REYNOSO : Merci beaucoup Michele.

Encore une fois, nous vous donnons la parole pour les questions pour les panelistes. Numéro six, numéro cinq ensuite. Très bien, numéro six.

MILTON MUELLER : Milton Mueller de Georgia Tech.

Consolidation et concentration, ce sont des termes qui sont soulevés dans les discussions sur le DoH mais pas dans le DoT si j'ai bien compris. Mais lorsqu'on fait une analyse économique, ce sont des noms très spécifiques. Est-ce que la concentration et consolidation, c'est quelque chose de mauvais ? Parce qu'ils

donnent le pouvoir de définition des prix aux fournisseurs. Si je comprends bien, les gens ne payent pas lorsqu'il y a concentration et distribution. Et cette concentration, est-ce que cela mènera à certaines préoccupations ? Est-ce que vous pouvez nous expliquer ce qui va se passer dans le marché pour les services de l'internet ? Quel sera l'impact ?

VITTORIO BERTOLA : Ce n'est pas un problème de prix parce qu'actuellement, vous avez votre internet et votre FSI et cela fait partie des services. C'est plus un problème de concentration des informations et de contrôle.

Donc par exemple, si on promeut la protection de la vie privée mais si à la fin tout le monde utilise le même résolveur, le résolveur verra les informations. Donc potentiellement, ce sera une perte en matière de protection de la vie privée.

MICHELE NEYLON : Je crois, Milton, comme Vittorio le disait, ce n'est pas une question de prix. C'est plus la question de savoir si l'internet fonctionne parce qu'il est distribué. C'est un réseau de réseaux. Tous les FSI peuvent en fait avoir leur propre résolveur, résoudre les réseaux, nous pouvons tous avoir notre propre résolveur. Si

vous concentrez, vous perdez cette stabilité, cette résilience. Il y a ce potentiel que la résilience disparaisse.

Et également, il y a la question... en fait, vous avez énormément de données dans le trafic DNS. Ce n'est pas uniquement ce qu'il y a mais également être qu'il n'y a pas. Les gens cherchent à aller quelque part dans une destination qui n'existe pas et c'est cela en termes d'argent la question qu'il faut se poser.

ALEJANDRA REYNOSO : Micro cinq.

ORATEUR NON-IDENTIFIÉ : Il y a une certaine confusion. Lorsqu'on parle de DNS au niveau du navigateur, c'est donc le niveau usager. Alors qui applique les politiques ? Comment peut-on clarifier au niveau des politiques ce qui se passe ? C'est la question que j'ai.

TIM APRIL : Votre question, c'est qui définit la politique qui est implémentée dans le navigateur. C'est cela la question ? Et bien cela dépend du fabricant du navigateur et cela dépendra aussi du feedback des usagers qui l'auront utilisé. Il n'y a pas de mécanisme ou de politiques qui les forcent à faire quoi que ce soit. En fait, ils peuvent faire ce qu'ils souhaitent.

ALEJANDRA REYNOSO : Merci.

Numéro trois.

EDUARDO DIAZ : Est-ce que c'est possible, si je deviens une grande société avec un grand résolveur, que je puisse commencer à vendre ou à proposer un domaine de premier niveau sans m'adresser à l'ICANN ? Et les autres résolveurs pourraient me contacter s'ils ne trouvent pas la racine ? Est-ce que c'est possible ?

TIM APRIL : C'est possible du point de vue technique. Il n'y a rien qui vous empêche de le faire.

DANNY MCPHERSON : Et je pense que le DoH et le DoT ne changent rien par rapport à cela.

TIM APRIL : Oui, c'est exactement comme le .onion.

ALEJANDRA REYNOSO : Numéro quatre.

FRED BAKER : Ce qui m'inquiète, c'est le routage internet. Et je vais parler d'un cas que vous connaissez sans doute bien. Il s'agit d'une entité nationale que je ne vais pas mentionner de nom.

Mais le problème, c'est que souvent – c'est également un problème pour les entreprises –, les sociétés imposent des informations, des modules de sécurité et elles le font en refusant l'accès à un certain nombre de noms d'une manière ou d'une autre.

L'entité à laquelle je pense, ces personnes ont décidé d'utiliser le résolveur Google et en fait, cette caractéristique a été empêchée. Il y a eu piratage du résolveur Google.

Au point où une solution de sécurité devient un routage de piratage, personnellement, comme je travaille dans la sécurité, je suis vraiment très inquiet. Ce qui m'intéresse, c'est vos commentaires par rapport à cela, donc.

DANNY MCPHERSON : Oui. Vous savez, le système de routage, c'est en fait une toile de confiance. Et certes, il y a la rumeur. Vous pourrez choisir de croire ce que quelqu'un vous dit, il n'y a pas d'autorité centrale. Il y a des techniques RPKI par exemple. Donc lorsqu'on utilise

une infrastructure, on devrait utiliser ces techniques pour sécuriser le système de routage. Mais je suis d'accord, je crois que le système de routage, à la base, est une réelle préoccupation en matière de sécurité sur l'internet. Et tous les services en sont conscients et il faut effectivement s'en occuper.

TIM APRIL : Et il y a également un autre cas et j'aimerais le mentionner rapidement. Il y a en fait aussi le fait qu'il faut utiliser les DNSSEC et DANE. Donc il y aura validation du certificat par le DNS en utilisant les DNSSEC parce que les DNSSEC valident. La communication passe. Alors que si on est dans une zone où on a accès à quelque chose qui fait confiance au stockage, cela pose problème.

ALEJANDRA REYNOSO : Merci beaucoup,

Numéro six.

MARK SVANCAREK : Mark de Microsoft.

Par rapport aux questions à l'auditoire, qu'est-ce qui vous préoccupe ? Il y a le problème de la concentration du DNS, les

fournisseurs. Pourquoi est-ce que ce n'est pas la question affichée plutôt que ces protocoles ? Si justement le navigateur le plus populaire, par défaut si j'ai bien compris, ira au quad-8, vous avez donc cette gigantesque concentration, quels que soient les nouveaux protocoles. Donc pourquoi est-ce que ce n'est pas la question qui vous préoccupe le plus ? Cela ne fait qu'accélérer la tendance. Donc je pense que ce devrait être un des points à l'écran plutôt que d'avoir des questions relatives aux protocoles. Merci.

TIM APRIL : Warren disait que Chrome ne va pas sélectionner le quad-8 par défaut. On peut le sélectionner mais...

MARK SVANCAREK : [inaudible]

TIM APRIL : Warren pourra me corriger si je me trompe mais si j'ai bien compris, Chrome devrait implémenter ceci de la manière suivante. Par défaut, si votre résolveur de système accepte DoH, il va l'utiliser comme chemin de résolution. Sinon, on retombe sur l'autre résolveur et ensuite, on va vers le résolveur choisi.

Donc on peut choisir le quad-8 ou alors dans un menu déroulant, on peut changer le défaut dans Chrome.

VITTORIO BERTOLA : Si vous me permettez d'ajouter quelque chose, il y a des questions de sécurité dont nous avons déjà parlé et qui existaient déjà lorsqu'un utilisateur fait appel au quad-8. La question, c'est que cela rend les choses comme une solution par défaut, ce qui rend plus difficile pour les usagers. Je suis d'accord que toute concentration est une source de préoccupations. Je suis content de savoir que Google n'a pas à faire ce déploiement maintenant mais on ne sait pas ce qu'il fera dans cinq ou six ans.

ALEJANDRA REYNOSO : Merci beaucoup.

Numéro cinq.

ROBERTO GAETANO : Roberto Gaetano, utilisateur d'internet.

Je suis suffisamment vieux pour avoir été témoin de l'époque où les logiciels étaient une poignée de solutions qui faisaient un peu tout dans différentes parties. Et ensuite, on a vu apparaître

une architecture avec sept couches, la couche transport, la couche physique, etc. Et le résultat a été la possibilité d'avoir des logiciels ouverts avec des solutions qui pouvaient être concurrentes pour chaque couche.

Avec ce type d'approche, DoH et DoT, est-ce qu'on ne revient pas en arrière vers ces solutions propriétaires en limitant la possibilité d'avoir des solutions qui rentrent en concurrence et que l'on revient aux années 1970 lorsqu'on appelait les solutions spaghetti ?

DANNY MCPHERSON : Oui, votre point est tout à fait juste. L'utilisation de ce type de système, au lieu d'utiliser les résolveurs minimum, etc., si vous voyez une fusion dans le chemin de résolution et que l'on a tout regroupé, il y a des implications au niveau des infrastructures, au niveau des usagers. Il y a plusieurs parties qui peuvent en tirer des bénéfices et il y aura aussi des perdants.

D'un côté, je comprends bien ce que vous dites mais d'autre part, je ne suis pas tout à fait d'accord parce qu'au niveau des applications des utilisateurs, vous aurez la possibilité d'utiliser l'infrastructure de résolution que vous voulez. Et cela peut influencer les opérateurs de réseau pour qu'ils mettent à jour

leur capacité. Autrement, l'usager reste captif et doit se fier à ce que l'opérateur décide de faire.

PETER KOCH : Je peux ajouter. Roberto et la personne précédente n'ont pas dit que c'est une espèce de silo et qu'on va un petit peu en arrière, oui. C'est une tendance qui n'est pas tout à fait liée à la standardisation des protocoles mais qui suit une certaine tendance.

La plupart d'entre vous ont beaucoup d'applications dans vos téléphones. Il y a eu de longues discussions sur ce que cela représente au niveau de la normalisation, la standardisation pour les infrastructures centrales parce que quand on utilise les applications, que font les différentes normes ou normalisations en dehors du HTTPS ? Alors cela fait partie d'un problème plus général. Ce n'est pas le seul élément mais il y a une tendance qui concerne les différentes infrastructures avec lesquelles travaille l'ICANN. C'est pour cela que nous avons voulu discuter de cela avec le public.

ALEJANDRA REYNOSO : Merci.

Numéro trois.

JÖRG SCHWEIGER : Je tire la conclusion que DoH ou DoT n'est ni bon ni mauvais, cela dépend du déploiement que l'on fait. Donc l'utilisateur aura un choix et donc ce serait bénéfique d'utiliser DoH. Mais il faut prendre en compte que quand l'utilisateur télécharge une application, le chemin de résolution reste enterré dans l'application.

En réalité, il n'y a pas de choix. Cette application appartient à un acteur majeur et il n'y a pas de choix en réalité. Est-ce que cela est lié au modèle de déploiement ?

VITTORIO BERTOLA : Bien sûr, cela a fait partie de discussions très énergiques qu'on a eues par rapport à ce type de protocole et la manière dont les gens s'en servent. Le point le plus important, c'est que l'on comprenne si et comment une discussion doit être mise en place pour en parler parce que si les implications laissent l'usager décider, il faut savoir comment il va configurer cela dans ses dispositifs, si c'est par défaut et si cela va impliquer que les problèmes disparaissent. Le problème, c'est comment et quand nous allons avec ces discussions. Il y a peu de gens ici appartenant aux fournisseurs de navigateur. Donc comment

pouvons-nous faire en sorte qu'ils puissent participer à cette discussion ?

ALEJANDRA REYNOSO : Merci.

Nous avons deux questions à distance s'il vous plaît.

ARIEL LIANG : Première question à distance de Christopher Wilkinson : « La concentration a été un problème depuis 20 ans avec les serveurs, serveurs de noms, FSI, DNS, etc. Pourquoi allons-nous dans la direction contraire ? Où est-ce que ces résolveurs seront logés ? Est-ce qu'il y a des implications au niveau des coûts ?

VITTORIO BERTOLA : Je voudrais dire tout d'abord que les plateformes de résolveurs peuvent être distribuées dans différents pays. Mais si la compagnie se trouve dans un pays spécifique, elle va relever d'une juridiction spécifique. Et je suis d'accord avec les problématiques qui ont été soulevées avec ces inquiétudes.

DANNY MCPHERSON : Je comprends que le système de racines est le système de résolution le plus distribué au monde aujourd'hui, du point de

vue géographique et du point de vue de la résolution elle-même. Je pense qu'on a travaillé dans le passé à ce qu'on appelle les hypergéants, des entités d'internet qui sont constituées à 95 % du trafic internet. Et si les FSI et d'autres ne protègent pas la confidentialité de la résolution, alors ces entités vont voir davantage de trafic dans leur serveur, ce qui aura des implications au niveau juridique aussi. C'est quelque chose que l'on voit apparaître maintenant. C'est très récent.

ALEJANDRA REYNOSO : Merci.

Deuxième question.

ARIEL LIANG : Deuxième question de Mike Bagley : « Est-ce que TLS permet de mieux *bypasser* le DNS ? Est-ce que cela n'augmente pas les risques au niveau de la sécurité ? »

MICHELE NEYLON : Oui. C'est la réponse courte, oui.

DANNY MCPHERSON : J'ai dit dans ma diapositive que la résolution DNS se passe dans le même protocole avec la même destination dans la couche

application où le trafic a lieu. Et tous ceux qui veulent manipuler doivent travailler dur pour manipuler ces données.

Mais très franchement, l'un des problèmes ici, c'est que certains gens manipulent les réponses DNS aujourd'hui, que ce soit un fabricant de navigateur ou autre. Vous pouvez manipuler les réponses et avoir un impact au niveau économique. Il y aura des gagnants et des perdants par rapport à cela, bien sûr, mais les systèmes de sécurité peuvent intervenir et soit bloquer ces protocoles au niveau des entreprises, ce que font certaines entreprises, ou utiliser des proxy pour que l'on ne puisse pas résoudre au niveau natif ce type de requêtes. Mais cela peut être problématique au niveau de la sécurité également.

ALEJANDRA REYNOSO : Numéro quatre.

KAVOUSS ARASTEH : Merci beaucoup. Je vous avais dit que beaucoup d'entre nous ne comprenons pas ce qu'est le DNS. Moi, je ne veux pas parler au nom de personne.

Vous avez dit qu'il y a des difficultés au niveau de la sécurité. Donc nous sommes inquiets pour les implications au niveau de la sécurité.

Mais pour certains d'entre nous qui ne sommes pas nombreux, ce sont des problématiques nouvelles. Nous devons digérer tout cela, bien comprendre avant de pouvoir poser des questions, avant de répondre à la question de la sécurité et de la confidentialité ou de la protection de la vie privée. C'est une problématique qui est en plein développement, y compris la réponse numéro deux qui a trait à la mission de l'ICANN. Il faut d'abord qu'on puisse digérer toutes ces informations avant de pouvoir y répondre.

MICHELE NEYLON : Pour une fois, on est d'accord, Kavouss. C'est vrai que c'est quelque chose de très nouveau et certains d'entre nous avons fait des références à des termes qui ne sont pas connus de tous. Nous essayons d'encourager les gens dans différentes parties de l'écosystème à commencer à se poser ces questions, à se poser les questions les plus simples, les plus complexes, les plus dures avec différents niveaux de théorie ou d'hypothèses. Il y a certaines compagnies qui sont en train de déployer ces technologies. Et ces compagnies vont vous dire que tout ce qu'ils font, c'est pour le bien commun mais vous ne savez pas ce qui va se passer dans l'avenir. Parce que quelque chose qui commence comme quelque chose d'innocent peut évoluer et se transformer en quelque chose de différent.

Il est important, donc, de pouvoir se pencher dessus, commencer à avoir des discussions en dehors de cette salle aussi parce que ce sont des discussions qui ont eu lieu au niveau de l'IETF et ces discussions durent depuis trois, quatre ans, peut-être un peu plus. Cela a commencé avec quelque chose de simple, comment pouvons-nous rendre le DNS plus privé, et puis cela a évolué. Mais beaucoup de gens qui sont dans cette salle qui ne sont pas dans l'espace IETF et qui ne sont pas dans l'espace geek ne sont pas trop au courant. Maintenant que ces systèmes deviennent une réalité, le temps est venu de s'y pencher.

ALEJANDRA REYNOSO : Merci beaucoup.

Numéro cinq.

ANDY BATES : Je suis un des cofondateurs de quad-9. Mais question pour les panelistes est la suivante.

Je pense que nous ne voulons pas utiliser uniquement le DNS normal et c'est pour cela qu'on pense à d'autres solutions qui puissent apporter un peu plus de protection. Donc voulez-vous

qu'il y ait une consolidation de ces systèmes vis-à-vis de la cybercriminalité ?

VITTORIO BERTOLA : Chiffrer les choses, c'est quelque chose de positif. Si on peut résoudre certains problèmes de sécurité mais que l'on crée d'autres problèmes plus importants, alors on n'a pas progressé. L'aspect positif est de comprendre ce qui se passe, partager les politiques pour essayer de voir comment les politiques peuvent régir tout cela.

ALEJANDRA REYNOSO : Merci beaucoup.

Numéro trois.

WOLFGANG KLEINWAECHTER : Merci beaucoup. C'est la salle du GAC ici et vous avez dit dans une des diapositives que cela pourrait avoir des implications au niveau des cadres nationaux. Est-ce que vous voyez quel est le rôle des gouvernements ici et le rôle des forces de l'ordre ?

MICHELE NEYLON : Nous ne sommes pas chargés de ceci. D'accord ? Nous sommes une poignée de personnes à qui on a demandé de parler de cette question pour différentes raisons. Mais si vous voulez poser cette question, ce n'est pas à nous que vous devez l'adresser.

Vittorio va me contredire, bien sûr, mais c'est son rôle dans ce panel. Peter va me contredire aussi.

PETER KOCH : Pour la première fois de ma vie.

Excellente question. Je pense qu'il y a certains aspects de ce débat qui concernent les gouvernements. Il y a des gouvernements qui croient au blocage DNS qui interdit à certains usagers de pouvoir accéder à certains contenus.

Cependant, de l'autre côté, là où la résolution des domaines est utilisée pour éviter un accès accidentel à des contenus, on ne parle pas ici de hameçonnage ou des réseaux zombies, cela peut fonctionner. Mais rien ne dit que les fournisseurs de résolution – certaines d'entre eux offrent aujourd'hui des services de protection DNS, des pare-feux, etc. et ils offrent ces services.

Et pour répondre à la question de Milton, certains peuvent vous faire payer pour bénéficier de leur service de résolution où il y a des *black lists* par rapport à certains sites malveillants. Il n'y a

pas de raison pour que cela ne soit pas déployé pour certains fournisseurs dont nous avons parlé.

Donc on ne doit pas croire qu'il n'y a pas de difficultés. Et si vous croyez au blocage DNS, vous y croirez, y compris avec DoH ou avec DoT.

VITTORIO BERTOLA : Je voulais ajouter un élément. Je n'aime pas particulièrement le blocage DNS mais il est important de prendre une décision par rapport au blocage ou non de contenu. Il est important que ce type de décisions soit prises de manière démocratique et non pas par des compagnies ou des navigateurs. Donc je pense qu'il faut un débat là-dessus.

Il y a des compagnies qui disent qu'ils vont sauver le monde de la censure et cela m'irrite pour vous dire la vérité. Il y a des gouvernements qui peuvent être confrontés aussi à ce type de problèmes.

ALEJANDRA REYNOSO : Merci beaucoup.

Nous allons passer à la question quatre. Nous allons donc clore la file d'attente pour les questions.

SÉBASTIEN BACHOLLET : Je vais parler en français puisque nous avons des outils d'interprétation et des personnes très qualifiées pour cela dans la salle.

Donc je suis utilisateur d'internet individuel et je suis membre d'ALAC. Il y a un certain nombre de questions que je voulais poser qui ont été répondues. Je vais en poser deux.

La première. Quel va être vraiment le choix de l'utilisateur final dans tout cela ? Est-ce qu'il n'y a pas un risque de se retrouver dans la situation où nous étions il y a quelques années, d'être chez AOL, chez MSN, chez CompuServe – donc ce sera chez d'autres gens aujourd'hui – mais dans un couple qui fera le choix pour nous d'où se fait la résolution et par où on accède à internet ?

Et la deuxième question que j'ai, c'est, nous sommes à l'ICANN. Quelles sont les conséquences possibles sur le nommage, sur les serveurs racine et la façon dont tout cela va être géré dans le futur ? Est-ce qu'on peut imaginer que l'ICANN n'ait plus besoin d'exister puisque ces couples de résolveur serveurs pourront très bien décider qu'ils ajoutent dans leurs fichiers de nouvelles extensions ou ils en enlèvent, donc le bloquer dans un sens mais

aussi en rajouter dans l'autre ? C'est des questions qui nous semblent importantes.

Je suis d'accord avec ce que vous avez dit tout à l'heure, il est absolument indispensable qu'on continue à travailler sur ces questions-là. Il est dommage que la standardisation soit faite avant qu'on ait pu avoir cette discussion avec l'ensemble des parties prenantes. Merci.

MICHELE NEYLON : Sébastien, merci pour la question. Je crois que votre première question, nous en avons déjà parlé dans la partie questions et réponses. Certes, vous avez le potentiel de vous retrouver avec une situation où il y a quelques personnes qui choisissent ce qui se passe. Et j'ai mentionné tout à l'heure également le fait que vous avez l'opposé du blocage. C'est vrai, il y a ce risque.

Mais les protocoles, les normes sont des choses qui sont développées par des personnes de l'IETF et d'autres organes de normalisation qui ont ces discussions à ce niveau-là. Vous pouvez suivre ces discussions, elles sont ouvertes. Certes, il y a la barrière technique, ce n'est pas pour tout le monde. Il y a des normes qui ont un impact sur la vie quotidienne des gens et les gens ne savent absolument pas de quoi on parle parce qu'ils ne sont pas experts.

Donc les gens doivent être conscientisés, doivent avoir ces discussions. Mais déjà organiser cette discussion maintenant est quand même quelque chose qui est pertinent.

Je ne sais pas si quelqu'un souhaite ajouter autre chose.

TIM APRIL : Je voulais ajouter les technologies DoH et DoT, à la base, ne sont pas les coupables. C'est l'implémentation, la mise en œuvre, c'est là que les décisions seront prises. Tout ceci aurait pu être fait sans DoH ou DoT comme proposition de norme à l'IETF. Cela aurait pu être mis en œuvre par les vendeurs de navigateurs.

Et la raison pour laquelle c'est un sujet d'actualité, c'est que ce sont les normes qui ont été proposées et que maintenant, on parle de cet ajout de mécanisme de protection de la vie privée au début des requêtes de DNS, au début du cheminement.

S'il y a des blocages qui sont mis au déploiement, j'imagine que les gens sont assez intelligents à l'IETF pour trouver des moyens de contourner ces blocages, ces obstacles.

ALEJANDRA REYNOSO : Désolée de vous interrompre mais il y a encore une dernière question à distance et nous sommes en retard. Donc désolée, on

pourra toujours continuer la discussion dans le couloir après. Donc question à distance.

ARIEL LIANG : C'est en fait un commentaire que nous avons de Paul Hoffman à distance : « DoH et DoT sont de nouveaux protocoles, mais les applications et les systèmes d'exploitation on pu faire des choses identiques à ces nouveaux protocoles depuis 20 ans. »

VITTORIO BERTOLA : Je crois que c'est lui qui a écrit la norme DoH. Mais c'est vrai, il a raison.

ALEJANDRA REYNOSO : Merci pour ce commentaire.

Je vais maintenant résumer et terminer sur ce sujet d'actualité en vous demandant à chacun d'entre vous de nous donner très rapidement ce que, en quelques mots, l'auditoire doit retenir de notre présentation. Allez-y.

TIM APRIL : Je vais commencer. Comme je le disais il y a une seconde, DoH et DoT sont deux normes proposées à l'IETF qui n'ajoutent pas

de capacités techniques au système de noms qui n'étaient pas possibles par des méthodes non normalisées.

Et la grosse préoccupation, à mon avis en tout cas, c'est que dans le cadre des conversations que nous avons actuellement, il y a beaucoup de choses qui dépendent de la mise en œuvre des détails, que ce soit dans les applications, dans les résolveurs et autorités au fur et à mesure que nous mettons en place ces mesures.

VITTORIO BERTOLA : Mon message, c'est simplement continuons de comprendre. Même si c'est la première fois que vous tombez dans ces discussions, continuez de chercher. Il y a beaucoup de support, il y a des gens qui sont prêts à vous aider. Vous pouvez trouver ce dont vous avez besoin.

Restez impliqués également en tant que membres de la communauté à la discussion à l'IETF et dans d'autres endroits parce que les politiques vont être rédigées. Il est important d'avoir les contributions.

PETER KOCH : Les normes qui ressortent de l'IETF sont utiles pour le développement que nous voyons, mais ce n'est pas la cause

racine. Donc nous devons nous concentrer sur la cause racine et vraiment regarder dans l'ensemble globalement ce que cela veut dire dans l'environnement de l'ICANN, pour l'ICANN et pour l'avenir de la gouvernance de l'espace de noms.

DANNY MCPHERSON : Du point de vue opérationnel, je crois qu'il y a certes des questions mais il y a également des avantages du point de vue de la sécurité et de la protection de la vie privée. Alors le déploiement aura certaines implications.

Avec ma casquette SSC, le SSAC commence juste à considérer cette question. Nous considérons également votre feedback mais ce n'est pas évident de tout suivre. Tout n'est pas terminé à l'IETF mais on devrait en arriver à des normes. Donc à l'ICANN, toutes les personnes qui participent aux politiques peuvent aider par le biais d'avis au fur et à mesure que le travail est effectué.

MICHELE NEYLON : Vous m'avez donné la parole en dernier, Alejandra. C'est dangereux.

Il y a eu des questions très intéressantes et des commentaires intéressants. Donc personnellement, j'avais mon propre

sentiment par rapport à la technologie quand je suis arrivé dans la salle. Mais j'ai écouté les commentaires, les questions et en fait, j'évolue toujours dans mon point de vue. Donc cela veut dire qu'on est sur la bonne voie dans la conversation.

Le message que j'ai pour vous tous, c'est que si vous regardez la diapositive qui est à l'écran, il y a plusieurs points par rapport où vous pouvez trouver des informations sur la prochaine réunion IETF. Je crois qu'il y a privacy.org qui a des informations sur la technologie, il y a différents blogs de différentes sociétés également qui existent. Il y a des groupes, Accenture je crois a un document qui a été publié récemment. Donc lisez des informations et posez des questions. Je vous y encourage.

ALEJANDRA REYNOSO : Merci beaucoup.

La séance est levée. On applaudit nos panelistes.

[FIN DE LA TRANSCRIPTION]