KOBE – Atelier sur les DNSSEC (2 sur 3)
Mercredi 13 mars 2019 – 10h30 à 12h00 JST
ICANN64 | Kobe, Japon

JACQUES LATOUR : Bonjour. On est dans la deuxième partie de notre atelier. Il y a quatre présentations, les deux premières sur les DNSSEC et DNSSEC sur TLS et DNS sur HTTPS. Et puis on abordera la question du roulement de la KSK.

Warren Kumari sera notre prochain orateur.

WARREN KUMARI : Je m'excuse à l'avance. Ce ne sera peut-être pas gentil de ma part parce qu'on est dans un atelier de DNSSEC, mais ces DNSSEC prennent trop de travail, elles datent de 20 ans et il y a d'autres protocoles comme DNS sur TLD et DNS sur HTTPS, ces deux protocoles étant disponibles. Cela vaut la peine de faire tout ce travail pour mettre en place les DNSSEC ? Très bien, on va aborder la question.

En premier lieu, je peux vous dire que ce n'est qu'une introduction. J'ai simplifié des concepts et il y a même des simplifications un peu excessives. Je vais contrôler le temps de ma présentation pour essayer de ne pas dépasser le temps alloué.

En premier lieu, je dois parler du respect de la vie privée et de l'intégrité, à savoir deux questions différentes. On me demande d'approcher le micro mais je suis un peu petit. Voilà, je suis là.

La vie privée et l'intégrité sont différentes. Le respect vie privée indique de garder quelque chose en secret et de maintenir une information secrète.

Excusez-moi, j'ai un problème technique avec le micro. Je vais changer de micro. Voilà, ce micro fonctionne bien.

La protection de l'intégrité signifie s'assurer que l'information soit correcte. Je vais vous donner un exemple pratique pour bien comprendre.

Ici, on a un reçu d'une transaction dans un ATM. Vous avez en rouge le solde de ce compte bancaire. Il s'agit là d'une information que je ne veux pas partager avec tout le monde. Ceci n'exige pas de confidentialité, ce n'est pas la fin du monde si les gens connaissent le solde de mon compte en banque. Mais je voudrais m'assurer de vérifier que ceci soit vrai. Je sais combien d'argent j'avais, puis j'ai fait un retrait et voilà mon solde. J'ai besoin donc de vérifier que ce soit correct. Si la banque et moi, on a fait les mêmes calculs, le solde devrait être le même. Voilà donc la protection de l'intégrité ou la capacité de vérifier l'information.

Le respect de la vie privée, c'est mon numéro NIP pour accéder à la banque. Ce n'est que moi qui connais ce numéro.

Un autre cas par exemple, moi, ce qui m'intéresse, c'est l'intégrité des résultats ou pas la confidentialité ou le respect de la vie privée. Ce ne serait pas utile d'avoir la confidentialité parce que tout le monde veut savoir le résultat parce que la personne qui a gagné a été celle qui a été élue. Mais ce qui m'intéresse, c'est la confidentialité de mon propre vote à moi. Je ne veux pas que les autres connaissent pour qui j'ai voté, alors il faut avoir la sécurité des objets versus les canaux.

La sécurité des objets, c'est par exemple prendre des informations, les chiffrer et les encrypter pour qu'elles soient en toute sécurité. Par exemple, je peux écrire une lettre dans un code secret et ce serait une sécurité d'objet pour cette information. Mais la sécurité du canal implique de prendre cette lettre, la mettre dans une enveloppe, l'envoyer par la poste dans une enveloppe fermée. Alors c'est la sécurité de l'information dans ce canal en particulier.

Et quel est le rapport de tout cela avec les DNSSEC et le DNS sur TLS ? Les DNSSEC nous donnent la protection de l'intégrité. Ici, on a l'information publique, voici la signature pour ietf.org. C'est de l'information publique. Vous pouvez le vérifier, il n'y a pas de confidentialité. Cette information publique peut nous permettre

de faire des choses intéressantes, par exemple nous assurer que l'information n'a pas été modifiée dans les serveurs primaires ou secondaires du DNS ; deuxièmement, qu'elle n'a pas été modifiée absolument depuis l'internet à l'ISP. Et je m'assure là que l'ISP n'est pas interféré avec cette information. Je dois m'assurer que personne ne l'a modifiée. Et au cours de la dernière étape qui va de chez moi au ISP, elle n'a pas changé non plus, cette information dans mon réseau.

Il y a peu de temps, on a vu des routeurs, des foyers qui ont été affectés alors on a modifié les informations. Toutefois, les DNSSEC ne nous donnent aucun type de confidentialité. Donc cela veut dire qu'un attaquant qui est sur internet entre mon résolveur et l'internet peut voir exactement l'information que moi-même je regarde. Ceci n'est pas absolument vrai, cela veut dire qu'il y a quelqu'un qui regarde une information déterminée.

D'autre part, mon ISP peut dire qui regarde l'information. Alors il peut voir que moi je regarde un nom ou que je cherche quelque chose, un nom en particulier. Et ceci est applicable à l'attaquant qui est au milieu de mon foyer et de l'ISP. Ils peuvent voir ce que je chercher, et aussi dans mon routeur privé. Et l'attaquant peut voir ce que je cherche.

Ceci ne semblerait pas être un problème aussi grave que cela parce que ce n'est pas le trafic du DNS. Mais en réalité, il y a

beaucoup d'informations sur tout cela qui est vraiment importantes. Par exemple, si je cherche la page alcooliquesanonymes.org, il est probable que j'aie besoin d'aller dans une réunion, alors je ne suis pas si anonyme que cela. Et si je cherche par exemple le site des droitsdesgay.org, ceci montre un peu ma vie privée. Alors ce ne serait pas très souhaitable. Dans certains pays, on cherche des informations de certains partis politiques et nous savons que l'histoire ne finit pas bien. Dans tous les points où un attaquant puisse voir ce que l'on regarde, cet attaquant peut bloquer le trafic et empêcher que l'on cherche certains noms.

Là, on voit les questions du DNS dans le TLS sur HTTPS, etc. Tout cela nous donne la confidentialité, c'est-à-dire le respect de la vie privée. Alors on a la manière de trouver que dans mon routeur de la maison et dans la route avec mon fournisseur de service internet, je parviens à avoir la confidentialité de mes recherches internet.

Malheureusement, dans le résolveur, cette information est toujours visible et mon ISP peut voir ce que je cherche. Puis depuis le résolveur vers l'internet, cette information est visible et les attaquants peuvent la voir. Ils peuvent voir ce que l'on cherche.

L'IETF travaille pour améliorer cette situation de sorte à ce que l'on puisse faire l'encryptage de ces deux parties du circuit entre le résolveur et les serveurs autoritaires.

Dans certains cas, on voit que dans certains pays, il y a la censure. Voici une photo très connue du printemps arabe en Turquie. On a bloqué l'accès aux résolveurs locaux. Et la Turquie a bloqué une série de sites web que les utilisateurs voulaient voir ou accéder. Voilà, ceci, on l'a inscrit sur un mur justement pour que les utilisateurs changent les données de leur DNS. Ceci a marché pendant quelques temps mais plus tard, cela a été également bloqué.

Là, on voit le fonctionnement de cette technologie, on peut faire l'encryptage depuis notre foyer. Puis on passe à l'ISP et on se trouve dans un résolveur public à l'étranger. Et à vous de décider quel sera le résolveur que vous avez utiliser. Malheureusement, votre consultation est toujours visible et à la fin, elle sera chiffrée aussi. Voilà.

Le DNS sur TLS gagne dans la confidentialité mais on ne peut pas protéger la modification des registres dans le serveur de DNS avant l'envoi. Alors si les serveurs de noms secondaires ne sont pas gérés par vous-même, vous devez faire confiance à ce que personne ne les ait modifiés. Il y a une protection pour que quelqu'un protège les données dans le résolveur peu importe le

résolveur que vous utilisez, mais si vous n'utilisez pas DNSSEC, vous pouvez toujours voir l'information.

Donc c'est bien de se demander pourquoi ne peut-on pas avoir les deux technologies. Et ben ici, vous voyez le résultat auquel on parviendrait si on utilisait le DNSSEC et le DNS dans quelques uns de ces protocoles. On parvient à la confidentialité dans tout le parcours de l'information et aussi un degré important de protection de l'intégrité de l'information. On peut donc vérifier qu'on est parvenu à la réponse que l'on cherchait spécifiquement. Les DNSSEC donnent une certaine protection et le protocole DNS sur TLS donne une autre protection différente. Alors pour parvenir à une protection totale, il faudrait utiliser les deux technologies. Ceci peut sembler comme beaucoup de travail à faire mais si je veux avoir un niveau de sécurité optimal, je dois utiliser les deux technologies.

Et maintenant, si vous avez des questions, je suis à l'écoute.

RUSS MUNDY : Merci de la présentation. J'ai une question mais avant cela, je voudrais demander à tous les participants que pour la transcription et pour les interprètes vous disiez votre nom avant de poser la question.

Quand on combine ces deux technologies, quels seraient les possibles désavantages en plus de la difficulté ? Parce que c'est difficile, cela exige du travail.

WARREN KUMARI : Tout d'abord, il faut travailler beaucoup plus. À chaque fois que l'on ajoute une couche de sécurité, on ajoute un risque de défaillance. Alors si on travaille avec les deux technologies, on ajouter deux possibilités de défaillance et il y a plus de probabilités que quelque chose ne marche pas bien. Mais vraiment, le risque vaut la peine. Si ces deux technologies existent, il y a des raisons.

Je ne sais pas si j'ai répondu à votre question.

JACQUES LATOUR : J'ai une question sur le DNS sur HTTPS. Ceci ajoute un mécanisme pour vérifier l'intégrité du DNSSEC ?

WARREN KUMARI : Non. On a deux types de serveurs. Pensons comme dans un VPN, un réseau privé virtuel. Dans ce cas, une fois que le DNS passe par TLS, on ne peut pas modifier l'information en cours. Ce que l'on peut modifier, c'est juste au point de départ dans le résolveur.

Je ne sais pas si j'ai répondu à votre question. Je vois votre expression et je ne suis pas sûr d'avoir répondu.

JACQUES LATOUR : Alors à Firefox par exemple, on ne valide pas le DNSSEC ?

WARREN KUMARI : Non, d'après ce que je sais, non.

JACQUES LATOUR : Il faut travailler à cet égard.

WARREN KUMARI : Oui et je crois que c'est raisonnable d'avoir DNSSEC et DNS sur TLD. Vittorio va faire une très bonne présentation de DNSSEC sur HTTPS. Et il faut voir si l'on fait confiance à son fournisseur de service internet. Cela, c'est une question importante aussi.

JACQUES LATOUR : Merci Warren.

Il y a une autre question dans la salle.

ORATEUR NON-IDENTIFIÉ : Cela m'a pris quelque temps de me rendre compte que l'un des principaux avantages du DNSSEC, c'est que l'on ne se préoccupe

plus pour l'origine des données. En fait, cela permet d'avoir une certaine technologie dans le DNS. Mais si la signature des DNSSEC est valide, on ne se préoccupe pas pour la racine, d'où vient l'information.

WARREN KUMARI : OK. Une des questions que nous donnent les DNSSEC, c'est de pouvoir travailler avec DANE et des mécanismes similaires. Pour ces mécanismes, il faut s'assurer vraiment que l'on a obtenu la réponse que nous cherchions. On ne veut pas faire confiance au résolveur pour qu'ils prennent cette décision en matière de sécurité pour nous. Et cela permet de créer la protection de l'information entre le titulaire et vous-même. Et nous ne voulons que personne ne soit sur cette route.

ORATEUR NON-IDENTIFIÉ : Alors cela permet certaines routes peu fiables et compliquées. C'est comme le protocole HTTP où l'on ne préoccupe pas de ce qui se passe u milieu si l'information correcte arrive.

ORATEUR NON-IDENTIFIÉ : Le DNS sur HTTPS permet de valider le certificat et on pense que l'on parle au serveur DNS qui croit être le serveur correct. Mais ce qui importe, c'est la sécurité de l'objet, n'est-ce pas ?

JACQUES LATOUR : OK, très bien. Merci à tous.

On a une question de Geoff Huston, un participant à distance. « Il y a une différence entre le TLS comme transport d'une transaction DNS ou pour utiliser comme objet d'HTTP ? »

WARREN KUMARI : Il y a une différence mais je crois que cela prendrait trop longtemps de répondre ici, à moins que quelqu'un souhaite répondre à cette question.

JACQUES LATOUR : On va écouter maintenant la présentation de Vittorio. Merci Warren de votre présentation.

[Applaudissements]

Notre prochain orateur, c'est Vittorio Bertola de Open-Xchange.

VITTORIO BERTOLA : Pendant que ma présentation est projetée, je dirais que plutôt qu'une présentation, il s'agit d'une série de réflexions qui me sont venues à l'esprit la semaine dernière sur ce débat entre DNSSEC versus DNS sur HTTPS. Je reconnais que l'orateur précédent a fait un excellent résumé. Nous sommes tous

parvenus à cette conclusion que nous avons besoin de ces deux choses-là parce que ce sont deux choses différentes. Lorsque nous parlons avec des gens qui ne savent pas autant de chose à propos du DNSSEC, ces gens-là pensent que l'on n'a pas besoin des deux. Et il se peut que l'on ait un certain mérite là. Donc quelle est la différence entre les deux ? Je vais rapidement exposer les points suivants et je vais passer sur ce que Warren a déjà dit.

La différence entre DNSSEC et DNS sur HTTPS, il s'agit de deux choses différentes depuis la conception et à partir du moment où ils ont été conçus. Apparemment l'une des conditions clés, c'était la manière de trouver l'intégrité sans avoir à mettre sous encryptage la communication, donc il faut tenir compte surtout de la charge informatique. Donc nous pouvons nous demander pourquoi on n'a pas utilisé l'encryptage pour les communications comme cela se fait maintenant. Et bien parce que c'est un modèle qui existe depuis moins longtemps. À l'époque, ce n'était pas une tendance en vigueur. C'est ce que m'ont dit certaines personnes.

Voyons un peu comment cela fonctionne. Cela nous dit que nous pouvons faire confiance à la réponse. L'objectif est que le client reçoive des données fiables, qu'il pourra faire confiance au fait que ce qu'il reçoit n'aura pas été altéré sur toute cette route ; disons que cela accorte une sécurité à l'objet.

DNS sur HTTPS, c'est différent parce qu'ils utilisent l'encryptage pour les communications. Toute la communication est sous encryptage et cela fournit une confidentialité. Bien sûr, le coût en termes d'informatique est plus élevé mais ce n'est pas un problème en ce moment. Et cela fournit une sécurité pour le canal, c'est-à-dire le canal utilisé pour communiquer avec le résolveur. Les gens disent donc : « Ce canal est sûr. Personne ne peut modifier ma réponse et cela me garantit aussi que la réponse n'a pas été altérée. » En définitive, c'est la même chose. Les gens ont commencé à se dire que ce sont deux mécanismes de sécurité différents mais le résultat final est que personne ne peut manipuler, altérer leurs réponses.

Alors pourquoi ne pas nous servir de ceci au lieu d'utiliser DNSSEC ? C'est une proposition vraiment attrayante parce que si nous disons que le niveau de garanti de la sécurité est le même, la confidentialité est plus grande et il y a plus d'intégrité qu'avec les DNSSEC, ce que les technologies ne fournissaient pas.

Les gens disent de toute façon que DNSSEC est difficile à gérer. Mais ce n'est pas tellement vrai. Dans cette idée, il y a un mensonge, un argument fallacieux. Ce que je veux dire, c'est que la différence se trouve sur la source à laquelle on peut faire confiance. Les DNSSEC vous donnent la sécurité en ce sens que la réponse n'a pas été altérée tout au long de la chaîne, à

commencer par la zone des serveurs de noms faisant autorité sur toute la chaîne. Dans le DNS sur HTTPS, nous avons la sécurité que du résolveur. La réponse n'a pas été altérée mais à partir du résolveur, la conclusion à laquelle nous pouvons arriver est la suivante. Si nous voulons avoir aussi bien la sécurité du canal que des données et l'intégrité ainsi que la confidentialité, nous devons avoir les deux systèmes.

Est-ce tellement vrai ? Il faut savoir à qui l'on peut faire confiance. La question pour ces deux modèles, c'est que la confiance sur la source de la vérité, c'est le système des serveurs racine dans le DNSSEC, à savoir que tout soit validé comme il le faut. C'est le système des serveurs racine alors que sur HTTPS, la source la vérité se trouve entre la main du résolveur ; la vérité est ce que le résolveur nous dit. Et le DNS sur HTTPS ne fait pas de validation par DNSSEC.

La question est de savoir quelle est la vérité à l'heure actuelle sur le DNS. Le DNS a été conçu comme base de données distribuée. Il faudrait donc dire qu'une réponse correcte du dark web du DNS, il n'y aurait qu'une réponse correcte et toutes les autres seraient fausses. Il y a beaucoup de gens qui parlent des mensonges du DNS et des technologies semblables. C'est compréhensible. Je ne présente pas d'objection à cela. Mais à vrai dire, même aujourd'hui, les réponses aux *queries* dépendent

beaucoup de ce que l'on fait et où, à quoi et à quel résolveur on adresse la consultation.

En définitive, la communauté du DNS dit qu'il ne s'agit que d'un chemin plus court. C'est la raison pour laquelle un résolveur nous envoie différentes réponses. La censure n'est qu'une partie très réduite des cas d'usage pour modifier les réponses à tous les niveaux. Pour la plupart des changements, il s'agit de question de sécurité et des noms locaux ou des choses comme celles-là. Le gestionnaire au niveau du résolveur inclut la sécurité pour tracer un périmètre pour s'assurer que les données ne sortiront pas de ce périmètre à ce propos. Il y a d'autres cas qui sont liés de manière volontaire. Il ne faut pas aller dans des endroits qui se trouvent en dehors du réseau, par exemple une société qui empêche les employés de se connecter sur Facebook sur les horaires de travail ou une famille qui veut empêcher ses enfants de jouer à des jeux qui ne sont pas appropriés. Il y a d'autres raisons pour la modification, d'autres motifs qui ne sont pas de la censure, une évasion d'impôts par exemple. Et les réseaux de distribution de contenu donnent des réponses différentes selon où l'on est et qui l'on est.

L'une des tendances que nous voyons ou une des questions que nous avons est de savoir si nous pouvons continuer à considérer le DNS comme une base de données distribuée. Est-ce que nous allons [lire] dans cette base de données où le DNS est devenu

beaucoup plus complexe ? C'est un service où le mécanisme anticipe un certain type de localisation aux différents niveaux de complexité de réponse. Si nous commençons à soulever ces questions, la question sur la vérité est une question très pertinente.

Et quelle est la vérité dans le DNS et quelle est la source de la vérité ? C'est une question qui est pertinente aussi.

Nous pouvons commencer déjà à nous occuper de savoir si nous avons besoin de cette intégrité sur toute la chaîne et dans le système des serveurs racine. On s'attend à l'heure actuelle à avoir confiance aux résolveurs. Il y a peu de systèmes qui fassent une vérification de DNSSEC dans le dispositif. La plupart d'entre eux font confiance aux résolveurs pour cette vérification. Si c'est le modèle, il faut faire confiance aux résolveurs et s'attendre à ce qu'ils ne nous mentent pas parce qu'on ne vérifie pas ce que l'on reçoit selon le DNSSEC.

Ce que Warren a montré, les images qu'il a montrées sur l'intégrité et la confidentialité sont très bonnes. Mais la condition ou le critère pour que la validation se fasse sur le dispositif est une exigence. Dans ce modèle utilisant DNS sur HTTPS, on se connecte peut-être sur un autre résolveur. Alors chaque application individuelle devra mettre en œuvre des validations. Il ne s'agit pas de les mettre en œuvre dans le

système d'exploitation mais chaque application qui fait une *query* aura besoin d'une validation. Ce serait super mais je me demande si c'est réaliste. Et si c'est le cas, comment pouvons-nous faire. Il se peut que ce ne soit pas non plus la manière de le faire. Si nous acceptons le modèle qui fait confiance aux résolveurs, nous avons ce DOH et cela nous permettrait de vérifier tout ce qui viendrait des résolveurs autoritaires. Mais il y a aussi le cas de perturbation (*disruption*) qui est une préoccupation du DNS sur HTTPS. Excusez-moi, je crois que les interprètes deviennent folles.

Ce cas de la perturbation (*disruption*) de DNS sur HTTPS est en moyen pour que l'opérateur de résolveur soit le propriétaire de l'espace de noms de domaine. Si nous allons dans un espace où le résolveur est la source de la vérité, le résolveur peut décider de ce qu'il veut nous raconter. Si je veux utiliser le système de serveurs de noms ou configurer de nouveaux TLD, on m'a dit qu'il s'agit d'une possilibité, même si ce n'est pas quelque chose qui ait été fait. Moi, je l'accepterais mais c'est l'un des soucis que l'on voit apparaître avec ce nouveau modèle de déploiement de DNS sur HTTPS. Mais c'est un autre cas qui peut se présenter.

Je disais donc que cette présentation n'est qu'une série de questions et de réflexions qui essaient de déclencher la discussion. Si nous nous mettons à la place des utilisateurs, nous faisons tous confiance au système des résolveurs de la

même manière que nous pouvons faire confiance aux constructeurs du navigateur favori. Les utilisateurs veulent vraiment que l'ICANN accepte les requêtes qui ont été validées ou une autre entité.

Et une autre question, l'un des thèmes de cet atelier était comment faire pour que les utilisateurs utilisent les DNSSEC. Est-ce qu'il y a une raison pour le faire ? Il se peut que l'on utilise simplement DOH et s'assurer que le résolveur mettre en œuvre DNSSEC.

Je crois qu'il faut discuter du fait que le modèle de DNSSEC régional soit valable, par exemple les critères de DNSSEC qui étaient pertinents il y a 15 ne le sont plus tellement maintenant. Il y avait différentes conditions et exigences il y a 15 ans, sur la confidentialité par exemple. Nous devrions donc réfléchir à ce qui suit. Au lieu d'ajouter davantage de protocoles dans cette pile de DNS, nous devrions peut-être réfléchir encore une fois aux critères et aux conditions et trouver quelque chose qui réponde à tout au lieu de mettre des petites modifications et nous finirons pas avoir quelque chose qui soit impossible à gérer. Voilà.

Merci.

JACQUES LATOUR : Merci. Est-ce que vous avez des questions ?

AFIFA ABBAS : Je m'appelle Afifa, du Bangladesh. Bonjour à tous. Ma question est la suivante.

Pour parvenir aussi bien à la confidentialité qu'à l'intégrité, Warren et vous-même, vous avez dit que nous avons besoin des deux choses. Ma question est la suivante. Il n'y a pas de raison où la deuxième option DNS sur HTTPS permet d'éviter toute altération du trafic. Est-ce que c'est raisonnable de se servir des deux ? Et si nous le faisons, est-ce qu'il y a des possibilités d'ajouter d'autres caractéristiques au réseau ?

VITTORIO BERTOLA : La réponse officielle est que bien sûr, il faut se servir des deux parce qu'ils sont censés répondre à deux raisons différentes. Nous devrions peut-être penser à différents thèmes. Mais il faut en définitive disposer des deux. Le DOH ou le DNS sur HTTPS doivent résoudre beaucoup de questions de politiques. Il faut d'abord avoir une connaissance des problèmes avant de donner les réponses.

En ce qui concerne la latence, cela dépend. L'une des questions de DNS sur HTTPS, il semblerait que cela promeut une certaine centralisation. Bon nombre des résolveurs dans les ISP locaux

vont se servir d'autres résolveurs à distance comme celui de Google, et cela va créer davantage de latence. Mais cela dépend de la connectivité parce que les consultations sur le DNS devront aller plus loin. Cela ne signifie pas nécessairement que cela sera plus lent. Cela dépend de la connectivité.

JACQUES LATOUR : Barry ?

BARRY LEIBA : Cela a été difficile de suivre votre présentation parce que vous parliez un peu vite. Mais en définitive, je crois comprendre que vous proposez un mécanisme hybride où le résolveur récursif vérifie DNSSEC à partir du serveur autoritaire et nous nous servons d'HTTPS pour gérer la communication avec le résolveur récursif. Et nous faisons confiance au récursif pour ne pas avoir à vérifier DNSSEC à cette étape-là. C'est ce que vous proposez ?

VITTORIO BERTOLA : Excusez-moi. Ce n'est pas quelque chose de fini, l'idée n'est pas tout à fait claire. Ce n'est pas quelque chose que je propose. J'analyse les différentes possibilités et je veux savoir ce que vous en pensez parce que c'est intéressant. Mais je crois aussi qu'il s'agit d'un modèle qui peut fonctionner. Cela soulève la question de la confiance qu'on fait aux résolveurs. Il faut

élaborer des politiques pour voir comment choisir le résolveur, travailler sur la supposition qu'il faut travailler avec un seul résolveur. Il y a des gens qui aiment distribuer leurs requêtes sur plusieurs résolveurs. Donc c'est très prématuré que de faire cette suggestion maintenant. Mais c'est quelque chose que nous pourrions considérer, en particulier parce que maintenant, nous parlons de questions de politiques avec le DNS sur HTTPS. Nous pouvons peut-être considérer différentes hypothèses et ne pas attendre à ce que 15 ou 20 ans de plus s'écoulent.

WARREN KUMARI : J'imagine que nous allons continuer à parler de cela au sein de l'IETF et dans d'autres forums.

Mais Vittorio a soulevé quelques thèmes. Et moi, j'aimerais bien parler de la question des navigateurs, le fait qu'ils doivent se servir de ces navigateurs. Google dira... Le moment venu, je me demande s'il y a toute une série de plans ou des questions qu'il faudrait altérer. Une chose importante consiste à ne pas étonner ou surprendre les utilisateurs. Si un utilisateur vérifiait et si le résolveur dont se sert l'utilisateur en fait un usage opportuniste, il faut savoir s'il n'y a pas de plan transposer le résolveur sans le consentement de l'utilisateur. Je crois que c'est quelque chose de très important parce qu'il y a un grand intérêt à savoir ce qui va se passer.

JACQUES LATOUR : Wes ? Ou enfin, je ne sais pas qui veut parler d'abord.

WES HARDAKER : Mon micro est ouvert, donc c'est moi qui ait gagné. Une présentation intéressante, toute une série de réflexions très intéressantes. Mais ce qui attire mon attention, c'est que les utilisateurs doivent faire confiance aux navigateurs. En fait, les navigateurs font confiance de manière transitoire à ceux qui leur donnent la résolution. Ce n'est pas les fournisseurs de navigation qui leur offrent cela comme par exemple une fois qu'il y a des accords ou des partenariats. Il y a eu des cas notables d'utilisateurs qui n'ont pas pu avoir des séances informées, de confiance. Et c'est intéressant parce que les utilisateurs font confiance à leur navigateur beaucoup plus qu'ils ne le disent parce que cette association peut fausser les requêtes. Nous faisons davantage confiance aux navigateurs que ce que vous suggérez potentiellement que l'on pourrait faire.

VITTORIO BETROLA : Avant la prochaine question, ce n'était pas fait pour forcer les navigateurs. C'est vrai, c'est l'approche de Google, mais c'est vrai. En définitive, toute cette architecture, en termes de

gouvernance et en termes technologiques, les serveurs de noms racine, c'est très compliqué. Si les utilisateurs sont obligés de voir à qui faire confiance, il se peut qu'on l'ont voit apparaître en premier lieu les navigateurs.

JACQUES LATOUR : Est-ce qu'il y a d'autres questions ?

STEVEN CARR : Je m'appelle Steven Carr.

Je comprends d'où vient toutes ces technologies mais il faudrait s'assurer que les navigateurs ne prendront pas le contrôle. Le DNS est le protocole sous-jacent. Faire tout cela sur le navigateur, c'est la solution incorrecte. Il y a de très nombreuses applications sur le système d'exploitation qui ne seront plus protégées avec cette technologie.

Comme Warren le disait, dans la mesure où les navigateurs auront le mécanisme pour déterminer si le système d'exploitation et sûr et qu'ils le renforceront, c'est bien. Mais si le navigateur prend le contrôle de la sécurité, je pense que nous ne devrions pas tomber dans ce piège parce que là, les utilisateurs auraient un sens d'identité qui est faux. Ils se sentiraient sûrs grâce aux navigateurs mais tout se qui se passe dans le système n'est pas sûr.

JACQUES LATOUR : C'est pour cela que nous abordons ce thème maintenant.

Je ne sais pas si vous voulez ajouter quelque chose, Warren ?

WARREN KUMARI : Apparemment, les applications seront de plus en plus capable de faire leur propre résolution du DNS. Que les gens pensent que l'idée soit bonne ou pas, il semblerait bien que ce soit la tendance. Et moi, je crois que cela est dû au fait qu'il y a des changements dans les applications et les gens décident que cela est bon. Je ne sais pas si c'est correct.

Un exemple de cela, il y a déjà assez longtemps que l'application de Netflix et d'autres s'occupent de leur propre résolution. C'est très facile de faire sa propre résolution. Et c'est un changement définitif dans l'architecture. C'est quelque chose sur quoi nous devrions faire des recherches et discuter. Il ne s'agit pas que des navigateurs versus les systèmes d'exploitation. Je crois que c'est les applications versus systèmes d'exploitation. Et il faut discuter de cela. Les gens qui rendront à l'IETF, il y aura une réunion spécifique sur ce thème et avant de débat, de très nombreux sous-thèmes.

VITTORIO BETROLA : Je suis d'accord et je partage votre préoccupation. Je suis dans l'IETF. Je suis l'une des personnes qui encouragent ce débat.

Un autre commentaire que je voulais faire, c'est que toutes les applications ne pourront pas faire de résolution par elles-mêmes. Si nous supprimons toute la sécurité au niveau du résolveur et nous la mettons du côté de l'application, le problème est qu'avec l'internet des objets, un réfrigérateur ne pourra pas faire de résolution. Il y a des problèmes graves en termes de résolution qui ne pourront pas être gérés par la résolution par l'intermédiaire des objets.

JACQUES LATOUR : Il n'y a plus de question. Nous remercions Vittorio de sa présentation.

[Applaudissements]

Maintenant, nous allons entendre la présentation de Duane Wessels qui parlera de l'analyse ultérieure au roulement de la KSK.

DUANE WESSELS : Merci Jacques. Je voudrais partager avec vous quelques données. Nous les avons collectées après le roulement de la KSK. Ici, vous voyez les dates clés jusqu'à aujourd'hui. Il reste

encore une date clé mais je voudrais me centrer sur ce qui s'est passé le 11 octobre, à savoir le jour du roulement de la KSK.

Le 11 janvier 2019, c'est le jour de la publication de la clé. Bien. Ces données viennent de différentes sources. D'une part, on voit du trafic de consultation au DNS vers les serveurs racine opérés par Verisign. Puis, il y a la signalisation d'étiquette pour ce même résolveur, conformément au document RFC8145.

Ici, vous voyez des graphiques de requêtes pour le protocole DNS qui est dans la racine. Ce graphique montre ce qui s'est passé un peu avant le roulement de la KSK et immédiatement après. Ici, il y a des millions de demandes ou de requêtes par jour. Avant le roulement, on voyait de 10 à 15 millions de consultations par jour et après le roulement, on a passé à 70-80 millions par jour. Tout au long des jours ultérieurs au roulement de la KSK, on a vu qu'il y a eu une augmentation de la durée de vie.

Dans ce graphique, on voit les adresses IP individuelles. J'ai voulu inclure cette information pour montrer que ces adresses IP ont différents types de comportements. Il y en a qui ont eu un pic d'activité puis cette activité a diminué. Alors cela n'a pas beaucoup aidé de voir les IP individuelles parce que le comportement était différent.

Là, on voit les changements au moment de la révocation. Au moment de la révocation, on voit une augmentation significative. Ceci a eu lieu pendant les 10 ou 12 jours après la révocation. Puis on voit ce qui s'est passé un mois après, une augmentation des données continue.

Et on voit maintenant que ces serveurs racine reçoivent 1 million de consultations par jour pour le DNSKEY ; cela veut dire que cela augmenté 100 fois par rapport à la période avant le roulement de la KSK.

Si ceci va continuer à augmenter et au fur et à mesure, le problème deviendra de plus en plus grave. Si vous pouvez communiquer avec les réseaux où ces consultations sont créées, il serait intéressant d'arriver aux motifs, aux causes, pour trouver une solution à ces problèmes et arrêter ce trafic de consultation.

Dans cette diapositive, on voit encore un graphique où l'on voit le comportement différent des adresses IP individuelles. Il y a une question. Ce changement est dû au grand nombre de réponses du protocole IPv6. Le nombre est de 1 425 octets en ce moment, bien plus qu'auparavant et bien plus que la taille minimale du protocole IPv6, à savoir 1 280 octets. Mais apparemment, ce ne serait pas la raison. On voit de 10 à 100 requêtes par seconde de certaines sources mais on en voit pour

l'IPv4 et pour le protocole IPv6 aussi. Cela semblerait donc une situation qui arrive immédiatement après le roulement et qui va disparaître. En anglais, ce serait *roll over and die*, faire le roulement et mourir. Cela fait dix ans, le registre régional RIPE a fait la maintenance de zone à .arpa, on a utilisé des ancres de confiance qui étaient configurées manuellement. Et lorsque les utilisateurs retiraient manuellement les clés de ces zones, il y avait des pics d'activité qui apparaissaient. À mon avis, ils sont très similaires à la situation actuelle.

Nous allons maintenant voir des graphiques qui nous aideront bien comprendre ces données. J'ai aussi quelques images que j'ai préparées. Mais avant cela, je voudrais mieux comprendre quelles sont les sources de consultation et quelles sont les consultations qui sont formulées. Il faut voir s'il s'agit des consultations de DNSKEY ou d'un autre type. Alors l'idée, c'est d'avoir des graphiques à deux axes. Sur un axe, on montre les consultations de DNSKEY et sur l'autre, les consultations d'un autre genre.

Voilà donc. C'est la manière dont on peut visualiser ce type de graphique. On ne voit pas clairement les données parce que toutes les données sont là à l'angle de convergence des deux axes. Alors on pourrait le faire autrement mais il y a beaucoup de superposition de données. L'idée est d'essayer de mieux distribuer les données de sorte à ce que les points qui

représentent des données dans le graphique soient toujours mieux distribués. De toute manière, il y a une densité d'informations énorme. Alors j'ai changé la taille des différents points qui représentent les données dans ce graphique et maintenant, on peut le voir de manière bien plus claire.

Maintenant que vous savez comment fonctionnent ces graphiques, vous devez vous apercevoir qu'il y a une ligne diagonale. Et je répète, chaque point représente une adresse IP ; chaque heure par exemple et chaque point qui se trouve au-dessous de cette ligne veut dire qu'il y a des consultations sur les clés contre les autres consultations. Il y a plus de consultations relatives aux clés, *key queries*. Vous allez voir que normalement, un résolveur de nom récursif se trouverait ici en bas ou à gauche où il y a un nombre très réduit de ce type de consultation.

Nous allons maintenant voir une autre partie de la présentation. Je veux afficher une image. Excusez-moi, je cherche l'image que je veux partager avec vous.

Ici, on a le graphique avec une animation. Cela bouge. C'est le roulement de la clé pour la signature de zone ZSK. En réalité, ce n'est pas le roulement de la ZSK. C'est plutôt la publication préalable de ces clés ZSK dans la zone, la clé pour la signature de zone. Vous allez voir qu'il y a beaucoup de petits points qui

bougent, qui dansent tout près de la diagonale. Et apparemment avant et après l'évènement, tout est tel quel.

Mais si l'on regarde plus en détail, on verra qu'il y a des petits points verts qui représentent IPv6 et les points violets représentent l'IPv4. Il y a des groupes de points verts qui représentent IPv6. Alors on fait une consultation pour arriver à la clé. Cette consultation est interrompue et puis on essaie encore une fois. Il semblerait qu'il y a deux consultations par source d'adresse IP et ceci se passe dans de nombreuses occasions.

Ce graphique animé vous permet de voir d'autres aspects intéressants. Si on regarde ici là où je signale, on voit ce point qui apparaît et qui disparaît. Apparemment, il y a des milliards et des milliards de consultations. Il y a un pic de consultations très bref et puis on a d'autres points qui apparaissent et qui disparaissent et qui se superposent constamment. Pour moi, c'est très intéressant de voir cela.

Là, je vous signale un autre aspect à tenir compte dans d'autres graphiques. Je crois que ceci est né en Corée mais je n'ai pas trop d'informations à cet égard.

Ce graphique animé correspond au moment du roulement de la KSK. Vous voyez qu'il y a une diminution de l'activité et l'activité reprend et continue d'augmenter. Peut-être après le roulement,

il doit y avoir eu un problème de résolution pendant quelque temps et puis l'activité normale a été reprise.

Je vais revenir au tout début et je vous signale cette partie de l'animation avec beaucoup de changements, beaucoup de sources de consultation qui sont devenues de plus en plus actives et ont commencé à envoyer des tas et des tas de consultations. C'est quelque chose très différent du moment que je vous ai montré auparavant.

ORATEUR NON-IDENTIFIÉ : Duane, pouvez-vous expliquer ce comportement des consultations entre tous ces clients ? Non. Par exemple les consultations de DNSKEY.

DUANE WESSELS : Vous parlez de la diagonale ? À vrai dire, je ne peux pas vous l'expliquer.

Mais si l'on pense au comportement attendu après un serveur de nom récursif, on verrait par jour une consultation DNSKEY par TTL, c'est-à-dire par cycle de vie. Tout ce qui est ailleurs dans ce graphique animé n'est pas normal. Il s'agit probablement d'un outil comme un serveur de nom caché. Mais ce que nous voyons ici ne reflète pas le comportement normal d'un serveur de nom récursif. Il s'agit peut-être d'un test, d'une mesure. Il y a

apparemment un grand nombre de sources de consultations qui font des mesures et je ne comprends pas très bien comment cela se passe.

JACQUES LATOUR : Cela, c'est pour les IP qui font quelles consultations ? C'est pour les IP historiques qui font ces consultations ?

INTERPRÈTE : Plusieurs orateurs non-identifiés parlent en même temps sans micro.

DANIEL MIGAULT : Pour ce qui est des consultations, par exemple au moment de .arpa et au moment de la situation que vous nous avez expliquée, on comprend la situation et la raison pour laquelle ceci a eu lieu.

DUANE WESSELS : Je vous répond dans quelques instants. Ce graphique animé montre la période autour de la révocation de la clé. Alors à la fin du roulement, on a beaucoup d'activités. La révocation a été un changement très abrupt, alors un grand nombre de ces sources de consultations ont enregistrée beaucoup d'activité, ont formulé beaucoup de consultations au niveau du DNSKEY. En

voyant ce graphique, je ne comprends pas très bien ce qui se passe et en conséquence, je ne peux pas l'expliquer.

JACQUES LATOUR : C'est peut-être un virus ou un bug.

DUANE WESSELS : Oui, c'est possible. Mais il faut voir de quoi il s'agit. Ces données augmentent et je les ai enregistrées jusqu'au 15 janvier. Je n'ai pas de données actuelles mais au cours des dernières semaines, on a vu une augmentation significative de ce genre de données. Ce que je vous montre, c'est justement le moment après la révocation.

[OLOF NORDLING] : Combien d'IP passent d'une partie du graphique à l'autre ? Plus de 1 000 ?

DUANE WESSELS : Je dirais plus de 1 000.

Je devrais continuer avec ma présentation. Je ne sais pas combien de temps il me reste. OK. J'ai inclus des images d'avant et après le roulement de la clé pour la signature de zone ZSK. On peut l'avoir comme future référence. Et je vais essayer de répondre à la question de Daniel.

Vous avez demandé ce qui s'est passé avec .arpa. À ce moment-là, on a publié un rapport sur ce qui s'est passé. Ce que l'on faisait, c'était la validation de DNSSEC. Il y a eu une défaillance parce que les clés n'étaient plus disponibles. Alors on a réessayé agressivement encore et encore une fois. Et cela était avant l'IPv6. Et je crois que c'est bien pire que ce que je vous raconte parce que l'idée est de faire ce qui suit. Par exemple, il y avait une requête .com. Il y avait deux serveurs de nom et toutes ces consultations étaient multipliées de manière exponentielle et on réessayait, réessayait les consultations de manière très agressive. À ce moment-là, on les gardait dans une mémoire cachée négative pour trois secondes seulement. Alors chacune de ces consultations a envoyé des dizaines, des centaines de consultations à la racine. Alors je crois qu'il y a eu un comportement similaire au cas d'autres technologies.

Enfin, je ne peux pas vous donner davantage de détails. Je crois qu'il y a d'autres problèmes là.

Je crois que dans ce cas, ils ont fait ce qu'ils pensaient correct suivant le document RFC pertinent.

DUANE WESSELS : Nous avons fait ce qui suit. Nous avons pris la liste d'adresses IP qui présentaient ses requêtes, on leur a demandé leur version .bind. Je ne fais pas trop confiance à ces données, mais elles

servent à titre d'information. Il y a différentes versions plus vieilles de bind. On n'a pas obtenu trop de réponses mais bon, il y en a qui ont été plus disposés à répondre. C'est finalement l'information que nous avons pu collecter.

Maintenant, je vais vous parler des données de signalisation d'étiquette clé. Ceci a eu lieu juste au moment de la révocation. Vous voyez en vert les sources qui indiquent la nouvelle et la vieille clé. En bleue, c'est marqué seulement la nouvelle clé. Alors on pourrait dire que ces chiffres si réduits indiquent que ceci a été configuré manuellement, que l'on a changé la clé manuellement. Dans cette ligne, nous marquons le moment de la révocation et nous voyons que dans une heure environ, la moitié de ces signalisateurs d'étiquette clé ont changé les données qu'ils envoyaient. En rouge, vous voyez ceux qui avaient seulement la vieille clé et n'ont pas changé le niveau d'activité après la révocation. On fait seulement attention au document RFC5011.

Il y a quelque chose d'intéressant aussi, comme par exemple voir la révocation de la clé de 2010 et de la clé de 2017. En fait, ce document RFC n'était pas trop clair. Les instructions n'étaient pas très claires pour ce qui est de la gestion de la clé révoquée dans l'ensemble des ancres de confiance. Il y en a qui disent qu'il y avait une seule clé révoquée dans l'ensemble des ancres de confiance. Ici, nous avons des données qui nous montrent

que nous avons encore des activités de 10 % dans toutes ces catégories.

Cette diapositive répète un peu ce que je vous ai déjà raconté. Les dernières diapositives sont un peu confuses mais ce que j'ai voulu faire, c'est combiner ces données et voir ce qui se passe avec les signalisateurs qui sont à ce niveau de DNSKEY dans les *top talkers* et voir les étiquettes clés. On voit les données que j'ai pu avoir au fur et à mesure. Et puis on voit ce qui se passe d'après les sources de consultation. Nous voulons dans certains cas qu'il y a davantage de stabilité. D'autres cas sont plus dynamiques. Nous recevons les rapports de temps à autre, alors ceci peut refléter l'activité dans des dispositifs mobiles.

Avec cela, je finis ma présentation. J'ai déjà répondu à quelques questions et si j'ai le temps, je vais encore répondre à des questions.

JACQUES LATOUR : Nous allons prendre les questions après Wes.

WES HARDAKER : Je m'appelle Wes Hardaker de l'USC ISI. Et je vais aborder la question de certaines données que nous avons eues sur notre serveur racine.

Moi, j'ai une addiction. J'adore créer des graphiques que je ne comprends pas, donc je partagerai avec vous mon addiction. J'ai déjà présentés des documents et j'ai obtenu des réponses. Je vais faire de même. Je vais présenter des graphiques que je ne comprends pas mais je vais aller vite parce que j'ai faim.

Je vais commencer par l'analyse d'une semaine de données, je vais parler de certains clients individuels qui me semblent intéressants. Il s'agit de données que nous pouvons mettre à disposition parce que nous aimerions bien voir la comparaison. Cette semaine de données, c'est entre le 9 et le 16 janvier de cette année. L'ensemble a été révoqué le 11 janvier. Voilà donc la semaine de données.

Comme vous voyez, le graphique a une apparence périodique. Il y a plusieurs points qui font des pointes un peu bizarres. J'en parlerai à la fin de ma présentation. Mais d'abord, je vais parler de la semaine de données. Mais comme la plupart du graphique, cela monte et cela descend tout le temps.

Voyons les requêtes au DNSKEY. La plupart des graphiques vont montrer cette ligne verte verticale du 11 janvier. Je ne suis pas très sûr pourquoi il y a cette chute. Une bonne partie de cette présentation a été préparée la semaine dernière et j'avais beaucoup d'autres choses à faire. Et on m'avait posé des questions déjà pour savoir pourquoi il y avait eu cette chute ; je

n'ai pas pu y répondre pour le moment. Moi, j'ai l'impression que ce sont des données qui sont cassées parce qu'il y a eu des gens qui ont fait moins de consultations après la révocation mais je ne sais pas pourquoi.

Voilà, c'est le nombre de consultations du DNSKEY par heure, donc des requêtes. Vous voyez qu'il y a une espèce de rampe. Les données à droite sont un tout petit peu plus élevées que celles qui sont à gauche.

Une autre chose que je cherchais, c'est ce que vous voyez là. Lorsqu'on fait une requête de la DNSKEY, qu'est-ce qu'on cherche ? La plupart cherchent la racine mais il y avait des requêtes sur d'autres noms populaires, tels que net et arpa.

Si nous analysons le comportement des résolveurs en général, il n'est pas habituel qu'ils demandent des clés différentes de celle-là. J'imagine qu'ici la raison pour laquelle on a demandé dlv.isc.org, c'est parce qu'il y a déjà deux ans que cela est tombé et l'on demande la validation. On ne devrait pas demander la clé en principe parce que c'est configuré mais je ne sais pas ce qui se passe là.

Lorsque j'ai commencé à ventiler toute cette information, lorsque j'ai divisé ces consultations et que je les ai attribuées à dans adresse individuelles pour voir d'où venait la plupart des requêtes, j'ai pu voir qu'il y avait une pointe le 11 janvier.

Chacune de ces couleurs représente une adresse différente. Certaines adresses ont une direction montante assez rapide et il y a des demandes de DNS en plus grand nombre.

Maintenant, voyons un peu les couleurs les plus intéressantes. Voilà celui qui a établi le plus de communications. C'est le numéro un et je l'appelle « Est-ce qu'il y a quelqu'un là ? Est-ce que nous sommes arrivés ? » Il y a quelqu'un demandé la clé à maintes reprises jusqu'au moment où personne ne lui a répondu et il quitté. Voilà le problème. Depuis le début, à droite, on peut voir le comportement normal. Donc quelqu'un faisait des recherches, des enquêtes. Pour le 16, en termes de ceux qui ont fait le plus grand nombre de requêtes, nous avons vu cet accroissement progressif assez faible au début. Cela a commencé à zéro et ensuite, ces requêtes duraient cinq minutes. Et ensuite, il y a un espace de montée et ensuite, il y a un niveau qui se tient assez constant.

Ceci était intéressant et se rapporte à ce comportement de sondage, enquête. Cette attitude de problème précoce, c'est-à-dire présupposer qu'il y a un problème et on voit apparaître la ligne sur le graphique et nous voyons que le problème se posait parce que l'on communiquait avant l'évènement. Il y a eu des gens qui ont eu des problèmes à la fin de la période. Je ne sais pas pourquoi. Parce que les résolveurs doivent résoudre au cours des deux premiers jours, faire une cache suivant la durée

de vie et l'on s'attend à ce que le problème se produise. Mais ce n'était pas le cas. C'est de cela que nous allons parler après. Il y a beaucoup de points dans la partie supérieure et beaucoup de points dans la partie inférieure pendant la même période de temps, parce que cela signifie que l'on pose beaucoup de questions ou que l'on fait beaucoup de requêtes pendant les premières cinq minutes et après, on ne pose pas de requête.

Le numéro 76 faisait beaucoup de requêtes au début. Ensuite, il y a eu le silence juste au moment de la période de révocation. Ensuite, ils ont continué à nous reposer des requêtes.

Je ne peux pas vous expliquer ces graphiques sont de la sorte. La seule chose que je peux faire avec vous, c'est de vous les montrer et de les partager avec vous.

Comment les choses se passaient alors que les gens allaient de pire en pire et que si l'on avait des patrons ou des modèles échelonnés, voilà l'un deux. La une grande population de zones dans le monde qui savent que si de nombreux résolveurs envoient des requêtes à une seule adresse, des choses comme celle que vous voyez se produisent. Ces espèces de marches disparaissent peu à peu au bout de deux jours. Mais pourquoi ? Je ne suis pas très sûr. Parfois, les choses s'améliorent. Il se peut qu'il y ait des choses qui soient interrompues ou parce que les

gens savent où se trouve le problème. Donc la courbe commence à descendre.

Voilà celui qui a eu le plus grand nombre de requêtes, le numéro un. C'est des requêtes de jusqu'à 15 000 toutes les 15 minutes. C'est un modèle très intéressant de pointe, je dirais une pointe par jour. Et la seule chose que l'on demandait ici, c'était la clé du DNSKEY. Je me demandais, mais qu'est-ce qu'ils demandent ? Non, il n'y avait que la clé qu'ils demandaient. Tout ceci apparaît après dans la partie du texte.

Voilà mon favori. Ce n'est pas parce que c'est 007 mais parce que cela a duré longtemps. Ensuite, il y a eu là une chute à des niveaux qui ne sont pas tout à fait déraisonnables, puis il a encore remonté. J'essaie de comprendre cela. Nous avons eu très peu de visibilité. Au lieu d'analyser les demandes originales, la plupart du temps, ce que l'on demandait ici, c'était la clé du DNSKEY. Mais il y avait très peu de visibilité sur les autres choses qui pouvaient se passer. On peut dire donc très bien : « Il y a deux jours, je me suis demandé ce qui se passerait si nous regardions les taux de requête, la vitesse minimale et la vitesse maximale. » Parce que comme je l'ai dit tout à l'heure, il y a des requêtes qui sont faites très rapidement et d'autres qui ne sont pas faites très rapidement. Donc voilà les vitesses minimales et maximales de l'heure. Vous voyez ce point vert géant à droite ayant une vitesse minimale, c'est-à-dire pour chaque point, il y a

un point violet et un point vert qui s'y rapportent. Il n'y a pas de référence. Excusez-moi, je n'ai pas pu... Il y a beaucoup de choses à améliorer ici mais ce que je veux montrer, c'est qu'il y a un espace significatif entre le minimum et le maximum. Cela indique que beaucoup d'ordinateurs font beaucoup de requêtes et il y a en a d'autres qui ne font pas de requêtes fréquentes.

Si nous prenons les valeurs qui sont en dehors du modèle ou du patron, il y a un grand nombre d'ordinateurs et ici, nous montrons ce qui a été classé à la vitesse maximale. Ceux qui sont en dessous sont ceux qui sont au-dessous de la vitesse maximale sur l'axe du X.

Lorsque j'ai préparé cette diapositive avec ce graphique, je n'avais pas encore fini l'analyse des données, mais j'ai remarqué qu'il y avait une tendance originale. Comme je le montre à gauche, cette espèce d'angle qui semble disparaître quand on termine les graphiques, une espèce de droite tombante. Je veux vous faire voir les points qui représentent la vitesse minimale qui se trouvent en dessous. Il y a ce patron de nombreuses requêtes et puis cette disparition aléatoire.

J'ai consulté ma source pour les données et tous ces graphiques concernent la seconde moitié de la journée. Parce que j'y ai réfléchi au début et je pensais qu'il y avait un problème avec les données. Durant la première moitié, je me disais qu'il doit y

avoir des problèmes. Mais je vois que cela s'est produit pendant la deuxième moitié et je continue à ne pas comprendre.

Voilà un autre graphique. Encore une fois, je n'ai pas de réponse pour ce comportement aléatoire. J'ai consulté une des universités qui fournissait les données et qui avait huit machines qui étaient en silence pendant la nuit. Les universités étaient toujours actives mais elles n'envoyaient des requêtes que pendant la journée. Elles ne faisaient que très peu de requêtes. J'ai écrit il y a deux jours au département informatique pour avoir une réponse aujourd'hui pour vous la présenter, mais je n'ai pas eu de réponse. J'ai contacté les personnes avec qui je communique mais elles n'ont pas donné de réponse.

Comme je vous le disais, tout cela provient d'un ensemble de données représentant une semaine. Nous voulons diffuser cet ensemble de données pour que vous ayez aussi l'occasion de l'analyser. Vous voyez en bas un graphique du site web Impact Cyber Trust, qui se sert de cette information à des fins commerciales. Je vais parler avec l'organisation ICANN pour savoir si cet ensemble de données est intéressant pour elle. J'imagine que c'est le cas. Comme je vous le disais, la semaine, c'était entre le 9 et le 16 janvier. Il y a plusieurs composantes intéressantes, non seulement le fait que cela est centré sur la question de la révocation de la KSK mais aussi sur le graphique de la partie inférieure, ce graphique ne représente qu'une

journée. Nous voyons qu'il y a des pointes dans les données sur le nombre de paquets qui ont été reçus. Il s'agit des graphiques du système de monitorage. La ligne inférieure représente la vitesse normale. Ces variations [inintelligible] depuis les enquêtes faites dans les adresses IP qui sont deux ou trois fois plus grandes que le graphique de requêtes que nous avons. Nous ne savons pas pourquoi ils le font. Nous avons parlé de cela avec d'autres opérateurs de racine et il semblerait que pour une question un peu singulière, ils se sont focalisés sur nous. Je ne sais pas ce qui se passe. Et les requêtes qu'ils envoient, c'est comme si c'était des ordures. Je ne sais pas, c'est comme si c'était des pourriels en quelque sorte. Donc contactez-moi si vous voulez en savoir davantage et nous allons essayer de trouver la réponse.

Il semblerait bien qu'il y ait des noms de DNSKEY. Il y en a qui sont codés sur Base64 mais c'est un paquet que je ne comprends pas. Je n'ai pas eu beaucoup de temps non plus pour l'analyser à vrai dire. J'aimerais bien que d'autres l'analysent et me disent ce qu'ils trouvent pour savoir si l'on peut attribuer cela aux propriétaires d'Amazon parce que l'on envoie tout ce trafic, parce que cela se passe depuis novembre sur un modèle ou un patron qui se répète toutes les semaines. J'ai contacté Amazon et ils m'ont dit : « Nous ne savons pas qu'ils le fait. » Et comment cela ? Nous avons utilisé deux canaux

d'Amazon et je n'ai pas trouvé de réponse. Nous voulons savoir donc ce qui se passe.

Je voulais savoir si vous avez des questions. Moi j'ai beaucoup de questions, bien sûr, mais je n'ai pas de réponses. Je voudrais savoir si vous avez des questions auxquelles moi je puisse répondre.

JACQUES LATOUR : Merci Wes. Il semblerait bien qu'il y ait une fuite au travers du DNS. Si vous pouvez organiser tout cela et le partager.

WES HARDAKER : Quelque chose d'ironique, c'est que l'on a parlé du fait que l'organisation devrait recueillir toutes ces données autour du 11 janvier. Et la réponse qu'on a eu : « non, cela ne va pas être très intéressant. »

JACQUES LATOUR : Nous avons dix minutes pour toutes les questions pour tous les membres du panel.

EDUARDO DUARTE : Eduardo Duarte, une question pour Duane. Sur la première animation, vous avez parlé du comportement de l'IPv6 mais

vous n'avez pas parlé du second. Il semblait bien qu'il y avait une opposition entre les deux.

DUANE WESSELS : Les évènements du KSK étaient adjacents aux évènements de la clé. Vous dites qu'il y avait une opposition dans tous les graphiques ?

EDUARDO DUARTE : Pour le second, c'était auparavant.

DUANE WESSELS : Bon, cela dépend de la réponse de la DNSKEY et du nombre de registres qu'il y a dans la zone. Dans le roulement, nous avons ajouté des signatures pour que la révocation puisse ajouter la nouvelle clé. Chaque fois qu'il y a une réponse de 1 280, cela fait augmenter le trafic par deux.

KATHY : C'est une question pour Wes de Geoff Huston : « Jusqu'à quel point voyez-vous que les réponses UDRP sont tronquées et les problèmes ultérieurs avec TCP ? Merci. »

WES HARDAKER : Nous l'avons dit il y a un certain temps et je ne suis pas sûr que ce que vous dites s'est produit il y a deux ou trois ans. Enfin, d'après ce que nous savons sur les opérations. Vous avez mesuré cela récemment ?

Je peux répondre de toute façon. Je ne pense pas qu'il y ait un grand changement entre UDP et TCP comme le graphique le suggère. Je ne sais pas, il faudrait que je le voie d'ici quelques jours.

KATHY : Geoff répond : « Non, nous ne l'avons pas mesuré récemment. »

WES HARDAKER : Oui, nous l'avons mesuré il y a un an et nous avons eu un commentaire similaire dans un forum semblable. Et j'ai dit que nous l'avions mesuré récemment. Nous pouvons vérifier si ce problème a été résolu. Mais avant le roulement de la clé, nous avons apporté une modification pour éviter de problèmes.

KATHY : Geoff dit aussi : « DNS A et J dit qu'il y a aussi une modification de 1 280 bits. »

JACQUES LATOUR : Quelle est la prochaine phase pour supprimer ?

WES HARDAKER : Le 22 mars, cela ne plus publié sur la zone.

Ces graphiques que vous voyez là, verts et violets, je les ai faits le 7 mars. Ils sont ultérieurs parce que je voulais voir si le problème était disparu mais bien sûr, le problème n'était pas disparu.

JACQUES LATOUR : Fred ?

FREDERICO NEVES : Frederico Neves, j'ai une question pour Duane.

Est-ce que vous avez contacté ces entités qui font le plus grand nombre de requêtes ?

DUANE WESSELS : Pas personnellement mais un autre opérateur du serveur racine est en contact avec les sources AS qui posent le plus de requêtes sur les adresses. J'aimerais bien avoir une explication de ce qui se passe. D'après mon expérience, ceci arrive, on les voit disparaître soudainement et nous n'avons jamais d'explications.

FREDERICO NEVES : De toute façon, les graphiques sont vraiment très bons.

DUANE WESSELS : Beaucoup de ce trafic se poursuit, donc nous devons être beaucoup plus actifs au moment de contacter les gens ; nous devons être alertes. Soyez alertes pour voir si nous pouvons vous donner une réponse pour faire le suivi des sources des données pour voir si nous pouvons comprendre ou déterminer ce qui se passe vraiment ici.

RUSS MUNDY : J'ai une question pour Duane. Avez-vous considéré projeter pour l'avenir ce que représenterait cette croissance du trafic d'ici six mois, d'ici un an, si les choses se poursuivent de la sorte ?

DUANE WESSELS : Je dois être honnête, non, nous ne l'avons pas fait. Mais ce serait une situation assez terrifiante pour ainsi dire. Si j'ai bien calculé, ces requêtes sur le DNS représentent 6 % du total du trafic et il faut en ternir compte me semble-t-il.

JACQUES LATOUR : D'autres questions ?

WES HARDAKER : Un commentaire final parce qu'on m'a écrit… On dit qu'une bonne partie de tout cela vient de DigitalOcean, d'Amazon,

d'AT&T, ce sont de requêtes génériques. Je ne sais pas si cela peut nous aider beaucoup, il y a une rotation générique.

JACQUES LATOUR : Merci beaucoup Wes.

[Applaudissements]

Kathy, pouvez-vous nous donner les instructions pour le déjeûner ?

KATHY : Oui. Le déjeûner...

[FIN DE LA TRANSCRIPTION]