KOBE – DNSSEC pour tous : un guide pour débutants
Dimanche 10 mars 2019 – 15h15 à 16h45 JST
ICANN64 | Kobe, Japon

WES HARDAKER: … Le DNSSEC pour tous, donc un guide des débutants. Voilà, aujourd'hui nous allons parler de ce qu'est le DNSSEC, comment cela protège votre utilisation de l'internet, et comment l'ICANN participe à ce processus.

Nous avons donc des personnages qui sont ici avec nous pour vous aider à comprendre le DNSSEC.

En attendant, je voudrais vous raconter une histoire sur le DNSSEC. Comment est-ce que le DNSSEC a commencé ? Le DNSSEC a commencé il y a très, très longtemps, donc 5000 années avant J.C, à l'âge des dinosaures. Cela a commencé avec Ogwina, voilà notre personnage principal. Ogwina vivait dans une grotte, tout près d'un grand canyon, et Og vivait lui aussi de l'autre côté du canyon. Et le canyon était très profond et très large. Et donc il fallait descendre et remonter de l'autre côté pour se rejoindre. Donc ils ne se parlaient pas souvent. Og et Ogwina ne parlaient pas souvent.

Lorsqu'ils se retrouvaient, lorsqu'ils traversaient le canyon, ce grand ravin pour se parler, ils se voyaient donc de temps en

***Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.***

temps. Et ils se disaient ; on pourrait peut-être communiquer avec des signaux de fumée. Donc rapidement ils se sont mis à communiquer avec des signaux de fumée.

Jusqu'à un jour où un autre homme préhistorique s'est mis lui aussi à utiliser des signaux de fumée en même temps. Et c'était très perturbant pour Ogwina parce qu'elle recevait des signaux de fumée des deux côtés et elle ne savait pas trop qui envoyait quoi.

Donc elle est descendue pour voir d'où venaient ces signaux de fumée. Ogwina et Og sont allés voir les sages du village. Et donc le sage, qu'on appelle l'homme des cavernes Diffie, donc Diffie est allé dans la grotte, dans le fond de sa grotte et il a trouvé de la poudre magique bleue. Une poudre magique qu'il a jetée dans le feu. Et, parce que ce feu était devenu bleu, Ogwina et Og pouvaient continuer à se parler, parce qu'Ogwina savait que la fumée bleue venait de Og, et seulement celle-là.

Bon, on a compris, vous avez compris ? C'était l'introduction du DNSSEC, vous avez tous compris ce que c'est. Maintenant on va vous donner quand même plus de détails.

Le concept derrière tout cela, c'est qu'il s'agissait d'identifier la bonne source des choses, et c'est exactement ça le DNSSEC.

Je vais revenir vers le DNS. On veut vous donner un petit peu une idée du concept de haut niveau du DNSSEC. Le guide du DNSSEC, si vous avez participé à cette réunion, on vous a certainement montré un organigramme tel que celui-ci. Il y a ici à l'écran, comme vous voyez, tous les TLD, les codes pays, donc les extensions géographiques, et ensuite vous avez les noms de domaine de deuxième niveau.

Aujourd'hui on va se concentrer sur bigbank.com.

La chose importante que vous devez savoir, c'est que l'ISP a un résolveur. Alors si le résolveur sait où est la zone racine », elle peut exactement savoir d'où viennent les choses. Alors bon, elle fait la recherche d'où est .com, etc., etc. Donc en très peu de temps elle peut savoir comment contacter tel ou tel niveau, savoir exactement où est la racine. Le résolveur donc trouve l'information.

Et malgré tout, il y a un problème. Il n'y a pas de sécurité dans toutes ces étapes. Il n'y avait pas de sécurité. Donc encore une fois, à l'époque tout se passait bien, il n'y avait pas de problème. Mais [inaudible], les noms étaient usurpés facilement, rapidement. Les caches étaient empoisonnés facilement aussi. On trouvait donc des réponses, mais pas forcément toujours les bonnes réponses.

Donc pour illustrer cela un peu plus, je voudrais amener devant vous les personnages que j'ai derrière moi qui portent des t-shirts blancs. Ils vont vous montrer un exemple de ce que fait le résolveur, ainsi que les ISP.

Et voilà, le monsieur qui est à gauche va faire des transactions bancaires avec bigbank.com. et il va faire ses recherches pour voir s'il peut trouver la bonne réponse.

RUSS MUNDY: Hey ISP, j'ai besoin de contacter bigbank.com, voilà le nom que je cherche.

WES HARDAKER: Ha, je ne sais pas où est bigbank.com est, je vais essayer de trouver la réponse je reviens vers vous.

Bonjour la racine, je voudrais aller à www.bigbank.com , pouvez-vous me dire où cela se situe ?

NON IDENTIFIE: Oui, je suis le serveur de la zone racine, vous cherchez donc .com. Pourquoi n'allez-vous pas au serveur 1.1.1.1 ?

WES HARDAKER: Oui, donc, allons-y. Bonjour .COM, je cherche www.bigbank.com, est-ce que vous savez où je peux y aller ?

NON IDENTIFIE: Je ne sais pas où est www, mais je sais où bigbank est, et c'est à 2.2.2.2.

WES HARDAKER: Ha bonjour, je cherche www.bigbank.com. Est-ce que vous savez où je peux trouver cela.

RUSS MUNDY: Oui, je suis igbank.com et je sais exactement où se trouve www.bigbank.com. C'est à 2.2.2.3

WES HARDAKER: Ha, très bien, je vais dire ça à mon utilisateur final.

RUSS MUNDY: Et peut-être voulez-vous cet argent ?

WES HARDAKER: Ha oui, alors apparemment vous allez à 2.2.2.3, et ça c'est www.bigbank.com.

NON IDENTIFIE: Merci.

WES HARDAKER: Bon, voilà, merci, merci à tous nos acteurs DNSSEC, on apprécie le sketch, on reviendra vous voir tout à l'heure. Attendez. Ha, ça va encore s'améliorer.

Donc, ce petit sketch est un peu similaire l'histoire d'Ogwina, quand elle parlait avec Og. Il y avait un résolveur qui essayait de partager un signal alors que quelqu'un venait et essayait d'usurper ce signal. Donc, le Kaminski, ce personnage, ce mauvais personnage, essayait d'usurper les signaux de fumée.

On va faire la même chose, le même sketch, et ça va être exactement la même chose, je vous le promets.

RUSS MUNDY: Allo, ISP.

WES HARDAKER: Bonjour.

RUSS MUNDY: J'ai besoin de faire un dépôt à ma banque avec bigbank.com. Est-ce que vous pouvez trouver pour moi ?

WES HARDAKER: Oui, alors c'est www.bigbank.com. Bonjour Racine, un de mes utilisateurs finaux cherche www.bigbank.com.

NON IDENTIFIE: Ha oui, je peux demander au serveur.com, à 1.1.1.1.

WES HARDAKER: Je vais lui demander. Alors serveur .com, je cherche www.bigbank.com.

NON IDENTIFIE: Je ne sais pas ou www est, mais je sais où est bigbank.com. Ça c'est à 2.2.2.2.

WES HARDAKER: Je vais leur demander. Un de mes utilisateurs essaye d'atteindre www.bigbank.com , vous pouvez me dire où c'est ?

NON IDENTIFIE: Ha bien sûr, alors ça se trouve à 6.6.6.6.6.

WES HARDAKER: Super, merci. Bonjour monsieur l'utilisateur, vous devriez aller à 6.6.6.6. C'est là où vous allez trouver www.bigbank.com.

NON IDENTIFIE: Ha bah très bien.

RUSS MUNDY : Je vais prendre votre argent, monsieur, merci beaucoup.

WES HARDAKER: Comme vous le voyez, il y a un problème. L'utilisateur ne sait vraiment pas à quelle réponse croire, et il croit la réponse qu'il reçoit. Voilà le problème avec les signaux de fumée, parce qu'avant il y avait deux signaux. Donc il faut choisir le bon. Et Ogwina ne savait quel était le signal qu'elle devait recevoir, qu'elle devait comprendre.

Donc pour revenir vers le concept de haut niveau de DNS, on a parlé de ce qu'il y avait en haut, en bas, et on a parlé de bigbank.com. Si vous parlez donc au mauvais résolveur, si l'ISP contacte le mauvais résolveur, cela cause un problème.

Le DNSSEC, cela résout ce problème. Le DNSSEC rajoute de la sécurité au DNS, une sécurité qu'il n'y avait pas avant. C'est une signature numérique. Cela vous dit que l'information est juste et correcte, et que la source est la bonne si vous voulez, que l'information est venue de la bonne source.

Donc les informations sont validées, ce qui est très bien, parce qu'ainsi nous pouvons savoir si l'information est sécurisée. On

peut donc utiliser le DNS pour savoir exactement ce dont on a besoin. Et on va vous montrer un exemple bientôt.

Le résolveur doit seulement savoir où se trouve le serveur racine, le DNSSEC c'est la même chose. Le résolveur doit savoir où sont les racines de zone et doit connaitre une clef. Chaque niveau signe la clef du prochain niveau, jusqu'à ce que la chaine soit complète. Si vous suivez cette chaine tout du long, vous savez exactement où vous allez.

Maintenant, l'avantage est celui-ci : avant Jo, l'utilisateur, ne savait pas quoi croire, maintenant il y a une validation qui se fait, donc on sait exactement qui croire.

On va donc refaire notre petit sketch pour faire les choses bien et ne pas faire intervenir le diable.

RUSS MUNDY: Hey, ISP, j'ai besoin de parler à bigbank.com. et j'ai besoin de savoir si la réponse que je vais recevoir est validée.

WES HARDAKER: Oui, attendez, je vais voir ce que je peux faire. Alors, racine, un de mes utilisateurs veut parler à www.bigbank.com pouvez-vous me dire où cela se trouve ?

NON IDENTIFIE: Je peux vous dire où est .com : c'est à 1.1.1.1 et voilà le certificat qui signifie que cette information est correcte.

WES HARDAKER: Ha bah je vais vous faire confiance. Nous allons maintenant vers le serveur .COM. Allo, alors un de mes utilisateurs veut aller à www.bigbank.com, pouvez-vous me dire où c'est et je vais vérifier votre signature avant d'y aller.

NON IDENTIFIE: Je ne sais pas où se trouve www, mais je sais où est bigbank, c'est 2.2.2.2.

WES HARDAKER: Je vais aller demander. Hey je voudrais l'adresse de www.bigbank.com, pouvez-vous me dire ?

NON IDENTIFIE: Alors bigbank.com est à 6.6.6.6.

WES HARDAKER: Attendez un peu. J'ai besoin du certificat, de la signature.

NON IDENTIFIE: Ha, je n'ai pas ça, je n'ai pas cette information.

WES HARDAKER: Je ne vous fais pas confiance alors.

Hello, est-ce que vous pouvez me dire où se trouve www.bigbank.com?

NON IDENTIFIE: En fait, je sais puisque www.bigbank.com est à 2.2.2.3, et voilà ma signature.

WES HARDAKER: Ha, ça a l'air d'être valide. Très bien, alors monsieur l'utilisateur, bigbank.com est à 2.2.2.3 et j'ai vérifié la signature et vous pouvez me faire confiance.

RUSS MUNDY: Je vois la signature, et je vous crois, maintenant je peux envoyer de l'argent.

WES HARDAKER: Est-ce qu'on peut applaudir nos acteurs ? Ils ont fait un très bon travail. On fait ça à chaque réunion. Quelques-uns d'entre vous ont déjà vu ce sketch ? HA oui, certains d'entre vous l'ont déjà vu.

Prochaine diapo s'il vous plait.

C'est équivalent à la fumée bleue dont on parlait tout à l'heure. Ogwina, finalement peut voir, peut comprendre d'où vient le

signal puisque la fumée est bleue. Et là on vient de parler des clefs qui sont utilisées pour signer chaque niveau.

Maintenant je vais passer la parole à mon partenaire de travail qui va vous expliquer pourquoi on a besoin de déployer le DNSSEC.

RUSS MUNDY: Merci Wes. Je suis Russ Mundy, et la portion que je vais vous expliquer aujourd'hui a à voir avec les choses que vous avez besoin de faire pour comprendre le processus.

Prochaine diapo s'il vous plait.

Un des aspects importants du DNS est celui-ci : souvent, les gens ne pensent pas que le DNS est utilisé par toutes les applications sur l'internet aujourd'hui. Donc lorsque les choses ne sont pas bien faites avec le DNS, ou qu'elles sont changées, ou pour quelque raison que ce soit il y a un problème, donc dans ces cas-là, les applications vont avoir des problèmes. Il y aura des problèmes de connexion, Jo l'utilisateur ne pourra pas parler avec sa banque par exemple. Donc il y a des questions fondamentales qui se posent quand on décrit le DNS.

Il est donc essentiel que toutes les applications fonctionnent et de comprendre comment les personnes, les différentes personnes attaquent le DNS.

Je suis ces activités depuis très, très longtemps moi-même, et franchement, je n'ai jamais vu un exemple où les gens attaquaient le DNS parce qu'ils voulaient changer le DNS. Ce n'est pas ce qu'ils recherchent. Ce qu'ils veulent faire, c'est qu'ils veulent avoir accès à des informations ou à des applications qui ont lieu après les recherches DNS. Ils veulent peut-être copier tous les emails, tous les courriels venant d'un emplacement spécifique, ils veulent changer les destinations du serveur, ils peuvent envoyer donc des courriels et donner des adresses fausses. Quand vous voyez beaucoup de courriels qui sont reçus par telle ou telle machine ne sont pas envoyés à l'endroit où elles doivent être envoyées. Les gens qui reçoivent ces emails ne font jamais la différence. Voilà, il s'agit d'une attaque de l'homme du milieu ou de l'intermédiaire.

Il y a quelques années, j'ai fait des recherches pour voir si ces cours, ces classes qui étaient donnés sur le sujet étaient encore sur internet. J'ai quand même trouvé une ou deux classes où les professeurs avaient dans leur cursus des classes sur le DNS, sur la sécurité sur internet. Des classes qui expliquaient ce qui était bon ou pas bon à faire sur internet. Il y avait des logiciels sur le sujet.

Il est donc très facile d'identifier les outils qui existent déjà ou les logiciels qui sont déjà sur le marché et qui peuvent aider pour mieux comprendre.

Alors, comment est-ce que le DNSSEC aide ? Comme vous l'avez vu dans le sketch, les questions qui sont posées par l'utilisateur passent par un processus de vérification pour savoir si l'information vient de la bonne source et si le contenu spécifique n'a pas été changé lors du trajet, lors du parcours.

Voilà un exemple de piratage. C'est un exemple un peu simplifié, pas aussi simple que notre sketch, mais comme vous voyez à l'écran, voilà la première recherche. La ligne pointillée, c'est la première recherche faite par l'utilisateur qui va vers le serveur autoritaire et qui revient au serveur récursif avec la réponse, ensuite cela revient vers l'utilisateur. Et, finalement, après tout cela, la recherche va vers le serveur web. Donc il y a du trafic, une circulation de réseaux que les gens ne connaissent pas en fait, c'est le trafic, la circulation DNS. Et c'est du trafic de courriel, ou d'applications telles que Facebook, etc. Ce sont toutes les transactions, toute la circulation de l'internet.

Ce qu'on a fait, alors les recherches qui arrivaient et qui étaient validées sur le DNS par les points de validation, on a fait des vérifications, et c'était particulier, on avait personnalisé cela. Et si on faisait des recherches et qu'on n'avait pas le DNSSEC, on voyait qu'il y avait un impact, parce qu'il n'y avait pas une vérification DNSSEC.

Donc ensuite, on a essayé de montrer ce qui se produirait dans ce cas, donc en cas de détournement. Donc voilà… Nous avons notre diable, avec sa grande cape noire qui arrive et qui donne une réponse. Et donc cela veut dire que Jo, utilisateur, avec cette réponse, s'est retrouvé sur le mauvais site web. La requête continue dans le site web, mais Jo l'utilisateur et sa machine ne l'ont pas reçu parce que la première réponse qu'il a reçue, celle qui venait du diable, était déjà arrivée dans sa machine et sa machine a dit : ha, c'est bon, j'ai une réponse, tout va bien, pas besoin de m'inquiéter.

Donc, avec le DNSSEC, vous avez un petit peu le même flux de paquets mais la différence c'est qu'avec la validation les paquets et les réponses DNS qui arrivent du diable ne sont pas acceptés par la machine de Jo l'utilisateur. Il y avait encore quelques flèches, mais voilà, c'est tout ce qui se passe.

Alors, la page personnalisée, à quoi ressemble-t-elle ? Et bien elle ressemble exactement à celle que je vous ai montrée tout à l'heure, la voici, la suivante. Donc, il y a eu détournement, et dans ce cas, c'est donc à l'époque où Steve Crocker était président du conseil d'administration de l'ICANN et Steve connait très, très bien le DNSSEC, il y travaille depuis longtemps. Donc nous avons mis un lien rigolo dans un autre endroit, qui a rempli une partie de l'écran que l'utilisateur verrait s'il venait sur ce site sans faire la validation DNSSEC. Donc en fait, on a détourné notre propre

site, nos propres informations pour démontrer ce qui pourrait se produire en cas d'attaque sur une page telle que celle-là.

Alors, lorsqu'on commence avec un résolveur vide, avec un navigateur vide, voilà ce que vous avez. Par exemple si vous allez sur [inaudible.com], ça je crois que c'était il y a 10 ans cet exemple à peu près, voilà à quoi ça ressemblait. Et donc maintenant c'est plutôt à ça que ça ressemble, donc beaucoup plus d'informations. Et ça, c'est uniquement pour une seule page web.

Alors, ce qui est important, vraiment, dans tout ceci, et la raison pour raison on fait le DNSSEC, c'est de s'assurer que le contenu de la zone est bon et qu'il reste bon au fur et à mesure de la circulation sur l'internet.

Autre illustration simple, là il s'agit d'une zone non signée, avec donc une requête, une réponse. Donc il y a nombre réduit d'étapes, et cela fonctionne très, très bien. Alors lorsqu'on ajoute le DNSSEC, qu'on utilise le résolveur et qu'on fasse une validation, qu'il s'agisse d'une FSI ou d'une entreprise, qu'il s'agisse d'une grande opération DNS, peut-être que vous avez un bureau d'enregistrement et que vous fournissez énormément de choses, et bien si déjà vous pouvez avoir propre système DNS et que vous incorporez le DNSSEC dans ces systèmes, et bien c'est relativement simple. Le plus gros enjeu c'est d'avoir un logiciel de

soutien qui incorpore les capacités DNSSEC. Et il y a eu énormément d'amélioration au fil des années par rapport à ça.

Alors, très souvent, la difficulté par rapport au DNSSEC c'est le problème le plus important, c'est lorsqu'on a son propre serveur de noms, mais il suffit d'installer un logiciel.

Alors si vous êtes une entreprise très importante, ce qu'il va falloir faire c'est le faire soi-même plutôt que d'envoyer ça chez un autre sous-traitant. Encore une fois, il y a extension d'une capacité, et dans votre organisation, en principe, cela existe déjà.

Alors si vous êtes utilisateur final, vous, en tant que personne assise dans cette salle, vous pouvez être la personne qui demande à ce qu'il y ait une validation DNSSEC chez votre FSI, chez votre fournisseur de services, quel qu'il soit. À ce moment-là vous n'aurez pas votre propre serveur de noms, la plupart du temps c'est quelqu'un d'autre qui s'en occupe. Et ces opérateurs sont justement les personnes à qui il faut demander qu'il y ait validation du DNSSEC, et qu'ils l'installent de manière à ce que personne ne vienne voler vos informations.

Alors, je l'ai déjà dit tout à l'heure, l'idée principale du DNSSEC c'est de s'assurer que les données de la zone qui sont incluses au début par les activités, que ce soit de la bigbank ou que ce soit du .COM ou autre entreprise, soient contenues dans le système et soient livrées par le système DNS à l'utilisateur final et qu'il n'y ait

pas de modification au milieu, entre-deux. Donc il s'agit vraiment de contenu de la zone, c'est ça qui est important. Et c'est là-dessus qu'il faut vraiment se concentrer, le contenu de la zone. Il faut que ce contenu arrive au bon endroit, et c'est tout aussi important que le reste.

À un moment il y a beaucoup de gens qui vraiment se concentraient sur : ha les utilisateurs de DNSSEC, c'est de la cryptographie, du chiffrement, c'est vraiment très spécialisé, il y a plein de choses à faire… Il faut simplement s'assurer que votre crypto soit géré correctement mais il y a des logiciels qui le font de nos jours.

Par contre, ce qu'il faut gérer, c'est le contenu. Le contenu doit être bien géré. Il ne faut pas qu'il soit modifié jusqu'à ce qu'il soit au serveur de nom. Et lorsqu'il est dans le serveur de noms, il faut absolument utiliser le DNSSEC pour valider.

Alors, maintenant, je reviens au diagramme de tout à l'heure. Il n'y a pas de grosses différences par rapport au diagramme de tout à l'heure. Comme vous le voyez, le concept revient à ajouter d'autres types d'enregistrements, c'est comme ça que cela s'appelle. Ils sont inclus au moment de la génération. Donc ceci est contenu dans le serveur faisant autorité, ensuite il y a validation au niveau du serveur récursif. C'est donc justement de

vérifier ce qui se passe, jusqu'à arriver à la racine, là où se trouve le bigbank.

Donc d'une manière générale, en terme de déploiement avec le DNSSEC, ce qu'il faut bien prendre en compte, c'est à quel point votre organisation, votre entité, est impliquée en termes d'exploitation de votre DNS actuel.

Si vous exploitez votre propre DNS, si vous avez vos propres serveurs de noms vous-même, et bien vous allez pouvoir effectuer ces fonctions supplémentaires pour fournir les signatures, la validation DNSSEC, au bon endroit.

Si vous n'exploitez pas ça vous-même, il y a par exemple beaucoup de grandes entreprises qui vont externaliser les capacités DNS à d'autres entreprises, par exemple PARSONS.COM, nous utilisons un fournisseur externe. Et une des raisons pour lesquelles on a choisi ce fournisseur externe c'est qu'en fait justement ce fournisseur externe utilise le DNSSEC. Donc si vous passez par un fournisseur externe, vous allez demander à ce fournisseur externe de faire le DNSSEC pour vous. Et n'hésitez pas à passer à un autre si le premier vous dit : ha je suis désolé, je ne savais pas que vous souhaitiez le DNSSEC, et je ne le fais pas. Et bien changez, il y en a d'autres qui le font.

Donc, cette activité est organisée par l'ICANN, par le comité consultatif sur la sécurité et la stabilité, le SSAC, il y a également

des membres du RSSAC, du comité consultatif sur la zone racine, qui sont là avec nous, et également par le programme DEPLOY360 de l'Internet Society.

Nous nous occupons de ce type de programme depuis longtemps. Je crois que là j'en suis arrivé à ma dernière diapositive, donc nous pouvons maintenant poser des questions.

WES HARDAKER: Merci beaucoup Russ. Nous allons demande au diable de se déplacer parmi vous avec le micro. SI vous avez des questions sur le fonctionnement du DNSSEC, s'il y a quelque chose que vous n'avez pas vu dans les informations présentées tout à l'heure, levez la main, Andrew va se promener et vous passer le micro.

ANGELA: Bonjour, je m'appelle Angela, je suis du Botswana et je fais partie de l'autorité de règlementation des télécommunications dans mon pays. Si la clef publique est détournée par le pirate, y a-t-il des mécanismes qui existent pour cette situation ? En cas de détournement de la clef, pour donc corriger la réponse.

WES HARDAKER: Excellente question. Je ne suis pas habitué aux bonnes questions. Donc tout à fait.

Que se passe-t-il si votre clef est compromise ?

Alors, plusieurs choses, il y a d'ailleurs d'autres experts dans la salle et n'hésitez pas si vous voulez ajouter quelque chose à ma réponse.

Il y a en fait deux clefs qui sont impliquées. Nous avons beaucoup simplifié les choses, mais il y a une clef publique et une clef privée. Vous avez parlé de la clef publique, donc cette clef on peut la donner à un peu n'importe qui. C'est la chose à faire, l'idée des clefs publiques c'est justement ça, elles sont publiques dont peut les donner à tout le monde. Par contre la clef privée reste privée. Si elle est compromise, eh bien oui, il faut immédiatement informer la société mère et dire : écoutez, il faut changer la chaine. Vous savez, on a vérifié tout le long de la chaine, donc en fait il y a une des personnes qui sera au milieu qui va être changée. Une nouvelle clef qui sera donnée à cette personne au milieu. Et donc cette clef privée sera changée.

Et donc vous pouvez faire ce changement assez rapidement. Il y a beaucoup de complexité avec ça, il y a différents éléments à prendre en compte, mais à la base c'est ça, vous dites à votre société mère, à la personne qui est au-dessus qu'il faut changer cette clef privée et ça peut être fait très rapidement.

Merci, y a-t-il d'autres questions après cette excellente question ?

SAVYO VINICIUS DE MORAIS : Je suis Savyo, du Brésil, je suis NextGen. Ma question est par rapport aux plus gros enjeux que vous avez par rapport au DNSSEC. En fait j'aimerais savoir pourquoi est-ce qu'il n'est pas plus utilisé sur l'internet.

WES HARDAKER: Alors, le plus gros enjeu, pourquoi est-ce qu'il n'y a pas plus d'utilisateurs qui l'utilisent ? Qui veut répondre à cette question ?

RUSS MUNDY : Et bien, vous savez, l'effort est continu en terme d'éducation, d'encouragement, sur divers forums, tel que celui-ci justement. Le travail qui a été effectué par le biais de différentes activités pour encourager les distributeurs de logiciels à avoir les bonnes structures, les bonnes capacités dans leur structure, essaie d'améliorer les choses. Donc nous essayons d'encourager les distributeurs d'application à épouser nos idées.

Alors, à mon avis, ce qui est utile, en particulier, c'est lorsque les utilisateurs, que ce soit des parties particuliers ou des entreprises, lorsque ces personnes disent : je veux mettre en place le DNSSEC. Certaines des fonctionnalités, certaines des sociétés, bureaux d'enregistrement, ne font pas le DNSSEC, et donc à ce moment-là il est difficile de le mettre en place si vous

travaillez avec cette société. Les opérateurs de registre, eux, le mettent en place de manière appropriée. Alors les utilisateurs finaux peuvent également demander aux distributeurs de logiciels de l'utiliser.

Donc accroitre la demande, le nombre de demandes de DNSSEC, à mon avis, c'est la plus grosse motivation. C'est ce qu'il faut manifester.

Divers programmes ont essayé de répondre à cette question. Mais en général, ce qu'il se passe, la réponse que l'on a, c'est que les utilisateurs ne le demandent pas.

Donc, notre objectif c'est que les gens comprennent de quoi il s'agit et notre rôle c'est également de vous convaincre que vous en avez besoin en tant qu'utilisateurs finaux.

NON IDENTIFIE : Un peu plus tôt, il y avait un diagramme qui montrait les résolveurs de validation. En termes de succès du DNSSEC ayant des moyens de mesure, c'est de voir comment sont signées les zones. Mais, ce qui est important autant que ça, c'est qui valide.

Si vous avez par exemple tous les domaines du monde qui signent, et bien peu importe si les serveurs récursifs ne valident pas ce qu'ils obtiennent.

Et il y a autre chose que je voulais dire, mais je ne sais plus ce que c'était.

WES HARDAKER: Oui, bonne question. On regarde constamment les statistiques, on essaie de voir un petit peu si le DNSSEC est en croissance, et si vous regardez les données, il y a une croissance du DNSSEC. Ce n'est pas aussi rapide qu'on le souhaiterait, évidemment.

Donc là c'est une page qui s'appelle stats.dnssec.tools.org, les données proviennent de Victor, qui connait très bien le DNSSEC, et comme vous le voyez, il y a eu un certain nombre, en fait des augmentations assez importantes récemment.

Nous avons fait le suivi de ce qui se passe en termes d'emails, et certaines des augmentations viennent de sociétés qui, de plus en plus, se sont mises à mettre tout en marche sur les serveurs de mail. Ils ont tout mis en route en même temps, donc voilà pourquoi on a ces bons en avant.

Mais effectivement, ce qui est utile, comme on l'a dit tout à l'heure, c'est que fait l'ISOC, ce qu'on fait aujourd'hui pour promouvoir le DNSSEC. Je crois qu'il y a eu 10 millions de domaines signés, mais en réalité, sur le .COM, il y en a beaucoup, beaucoup plus. On fait constamment de la formation par rapport à ça.

Y a-t-il d'autres questions ?

[COFY] : Bonjour, je suis Cofy, je suis de l'opérateur de registre du Ghana. Alors j'ai deux questions. La première, est-ce qu'il faut avoir des clefs privées qui sont changées régulièrement ou est-ce qu'il faut attendre qu'il y ait compromission avant de mettre en place le changement. Quelle est la bonne pratique par rapport à ça.

Deuxièmement, est-ce que le DNSSEC est une obligation pour être accrédité à l'ICANN, pour les bureaux d'enregistrement, etc.

WES HARDAKER: Oui, bonne question. Pour répondre à la première question, il y a deux écoles. Il y a des gens qui pensent qu'il n'est pas nécessaire de changer les clefs. Si les clefs sont suffisamment solides, pas besoin de faire une rotation régulière ou fréquente. Personnellement je n'ai pas envie de changer ma clef tout le temps.

Donc en général je ne les change pas souvent. Mais quand même, il faut savoir le faire, il faut avoir les compétences en place si nécessaire. Il y a beaucoup de gens qui font une rotation des clefs régulièrement, une fois par an, histoire de s'assurer d'avoir les compétences pour le faire.

Deuxième question, l'ICANN a certaines exigences par rapport à certaines entités. Par exemple, pour tous les nouveaux gTLD, il faut qu'il y ait le DNSSEC. Par rapport aux nouveaux bureaux d'enregistrement, est-ce qu'ils sont obligés d'utiliser le DNSSEC ?

RUSS MUNDY : Je n'en suis pas sûr. Je n'en suis pas sûr en fait que ça fasse partie de cet accord d'enregistrement.

WES HARDAKER: Alors, on va passer aux questions suivantes. Première ici devant.

[CORRY] : Je suis [Corry], je viens des États-Unis. J'ai une question par rapport au DNNSEC. Je sais que ça existe depuis un certain nombre d'années, mais récemment on a parlé du DNSSEC sur HTTPS ou TLS. Est-ce que c'est complémentaire ou est-ce que c'est en compétition ?

WES HARDAKER: Excellente question, vous êtes bien informé. Donc il y a plusieurs choses par rapport à ça. Non, c'est une question de complémentarité pas de compétition. DNSSEC signe les données, donc peu importe la manière dont c'est transporté, mais simplement l'enregistrement n'a pas été altéré. Il y a le DNSSEC

TLS qui est une spécification qui chiffre et qui dirige le trafic entre deux dispositifs. Et, par rapport à HTTPS, même chose. Et l'avantage principal de ça, c'est qu'il ne peut pas y avoir de problème de pare-feu.

Donc, il y a différentes raisons par rapport à ces technologies, mais la distinction la plus importante entre le DNSSEC et les deux autres c'est que le DNSSEC signe de manière à ce que quelle que soit la provenance vous savez que c'est authentique, il y a protection avec intégrité. Si vous faites TLS avec [inaudible], vous savez que la transaction est bonne mais vous n'avez pas l'historique de comment les données ont été obtenues.

Donc avec le DNSSEC, vous avez plusieurs cas, vous allez vous adresser à un fournisseur, mais vous ne savez pas nécessairement qu'ils ont à l'arrière vérifié les données.

Les serveurs faisant autorité ne font pas le DNS sur TLS par rapport à HTTPS encore.

RUSS MUNDY : Par rapport à l'atelier de mercredi, il y a un atelier DNSSEC avec une présentation spécifique sur ce sujet.

WES HARDAKER: Mercredi, c'est la bonne journée pour le DNSSEC.

RUSS MUNDY : Je fais un petit résumé. Le DNSSEC est là pour protéger les données. Les protocoles encryptés sont là pour protéger la confidentialité de votre recherche.

WES HARDAKER: Il y a une question de la salle.

[BALGISHNER] : Je viens du Népal. J'ai une question. Le DNSSEC protège l'utilisateur final. Est-il difficile pour vous de rendre le DNSSEC obligatoire ? Pour que tout le monde utilise le DNSSEC, est-ce que c'est difficile ?

WES HARDAKER: Oui, c'est dur parce que le monde est libre. Les gens dans le monde peuvent décider de l'utiliser ou pas. Il y a une phrase commune : il n'y a pas de police de l'internet, et ce n'est pas facile de faire la loi sur l'internet. Il faut choisir la technologie qui fonctionne pour l'un ou pour l'autre. Donc il n'y a aucune façon de forcer les gens ou les utilisateurs à utiliser le DNSSEC.

RUSS MUNDY : Oui, certaines organisations ont choisi de mettre en place des politiques de sécurité qui dictent des technologies de sécurité.

Donc certaines de ces organisations ont fait ce choix. Mais il n'y a pas une solution unique pour tout.

WES HARDAKER: Oui, il y a des gouvernements qui ont choisi d'utiliser le DNSSEC, que toutes leurs unités ou tous leurs organes utilisent le DNSSEC.

NON IDENTIFIE : Le DNSSEC perturbe le flux. Donc quand cela se produit, y a-t-il un ralentissement de l'internet ? Et de quel ralentissement on parle ?

WES HARDAKER: La vitesse que le DNSSEC produit pour ralentir l'internet. Oui, le DNSSEC c'est un peu plus lent, parce qu'il y a beaucoup de demandes qui sont faites à ce moment-là. Donc la chose critique qu'il faut comprendre c'est que le DNSSEC est inclus dans les caches. L'aspect sécuritaire est aussi en cache. Donc par exemple dans le cas de bigbank.com, vous voyez que tous les dossiers sont classés par dates si vous voulez. Donc ils ne peuvent pas tous être validés en même temps. Donc c'est une des caractéristiques intéressantes à ce sujet. Au début, la première personne qui va faire sa recherche, aura peut-être une réponse un peu plus lente que les autres, mais bon en général ça ne change pas grand-chose. Mais c'est une bonne question.

[CHRISTIANNE] : Je viens de la Côte d'Ivoire. Je voudrais savoir quelque chose. Je ne suis pas experte, donc ma question sera peut-être un peu stupide. Donc dans le cas où le DNS est piraté, ou usurpé, y a-t-il une procédure pour que le DNSSEC résolve le problème ? Et y a-t-il eu des cas où vous avez dû agir directement ?

WES HARDAKER: Oui, ça c'est un problème compliqué. Beaucoup de caractéristiques liées à la sécurité des systèmes… Dans ce cas-là les gens ne protègent pas leur système à moins qu'il soit trop tard.

Par exemple quand quelqu'un rentre dans votre maison et vol votre argent, c'est trop tard. Vous savez très bien qu'il faut mieux verrouiller ou protéger votre maison pour éviter que cela se passe.

Donc une fois que vous avez eu des soucis de sécurité, il est trop tard pour protéger votre DNS. Donc il faut déployer le DNSSEC avant d'avoir ce genre de problèmes.

ABRAHAM : Je viens du Nigéria. J'ai une question sur la mise en œuvre du DNSSEC. Doit-on augmenter le système ou maintenir ce qu'on a déjà en place avant donc de déployer le DNSSEC ?

WES HARDAKER: Oui, je ne sais pas si je vous ai bien entendu, il y a de l'écho sur la scène. Est-ce qu'il y a des requêtes pour un meilleur disque dur ou est-ce qu'on a besoin de plus de mémoire, de CPU, etc. pour mettre en place le DNSSEC ?

RUSS MUNDY : Il y a eu deux analyses qui ont été faites sur ce sujet. La plupart du temps, ces analyses ont été faites par les gens qui sont focalisés sur les TLD u niveau de la zone.

La conclusion a été celle-ci. La croissance normale du remplacement du cycle de disque dur qui devra être suivie est suffisante.

Malgré tout, quels sont les chiffres ? Si je me souviens bien, je pense qu'il y a eu un impact de 3 à 8 % sur le disque dur lors de la signature. Vous signez avant de charger la zone. Donc pour la validation, il s'agit d'à peu près le même niveau. Je pense qu'on en est à 10%.

Ça n'a pas un impact très important. Mais c'est quand même un facteur qu'il faut observer quand il s'agit de faire des programmes de mise à jour du disque dur.

WES HARDAKER: Oui, il y a une augmentation de mémoire, vous avez besoin de plus de mémoire. Donc pour résumer, je veux dire qu'il y a, sur 20 zones, je n'ai jamais vu de problème. Si vous êtes un TLD important, avec beaucoup de TLD, vous allez donc avoir à considérer ce problème là, mais pour les autres, non, je ne pense pas que ça va poser un problème.

[PAUL] : Je suis du Royaume-Uni. Quand on parle des politiques pour essayer de contrôler les violations du DNS au niveau des TLD, et bureaux d'enregistrement .

WES HARDAKER: Vous parlez de contrôler la performance ?

[PAUL] : Oui, quand on parle des violations des bases de données.

WES HARDAKER: Oui, il est très difficile de contrôler, du moins de surveiller si les choses sont mal utilisées. Je peux très bien contrôler à côté des TLD et voir si les informations sont les bonnes, mais les attaques n'ont pas lieu à cet emplacement-là. Donc il n'est pas facile de contrôler tous les ISP du monde. C'est une question très complexe que vous posez. Venez me voir après la réunion si vous voulez en parler plus en détail. C'est un problème difficile. Si on pouvait répondre à cette question, on pourrait arrêter tous les malfrats.

NON IDENTIFIE : Quant il s'agit de la demande du disque dur pour le DNSSEC, en République Tchèque, il y a une organisation qui publie des documents importants sur les serveurs DNS. Venez me voir après, je vous donnerai l'hyperlien, et vous pourrez voir là que l'impact sur le disque dur est vraiment négligeable, ce n'est pas très important, vous ne vous en rendrez même pas compte, à moins que vous ayez beaucoup de trafic sur un simple dispositif.

[BRONWYN] : Je viens d'Australie. Dans votre sketch tout à l'heure, vous aviez le résolveur qui validait le certificat à chaque niveau du domaine. Est-ce qu'il y a des mises à jour ou des changements de logiciel qui sont nécessaire au niveau du résolveur pour pouvoir soutenir,

appuyer, cette validation ? Est-ce que la résolution est faite pour le DNSSEC et pour toutes les étapes ?

WES HARDAKER: La plupart des nouveaux logiciels soutiennent, supportent le DNSSEC. Je ne me souviens plus de quelles sont les versions, mais ces logiciels soutiennent toutes les caractéristiques du déploiement du DNSSEC. Et ces logiciels, toutes les plateformes sont compatibles avec le DNSSEC. Je pense que le DNSSEC existe depuis assez longtemps, il n'y a aucun problème.

[CREJAN]: Alors, ma question. Au point de vue de l'ISP, y a-t-il des indicateurs d'impact qui indiquent que le DNSSEC est requis ?

WES HARDAKER: Oui, c'est une très bonne question. Les ISP sont ceux qui doivent développer un validateur, comme on l'a fait, vous l'avez dans le sketch entre chaque personne. Les ISP doivent parler, contacter la racine, les serveurs, etc., les TLD. Ils doivent s'assurer que leur logiciel puisse gérer toutes les transactions. Et on ne peut pas forcer tout le monde, dans le monde à utiliser le DNSSEC.

Ce qu'on n'a pas dit dans le sketch ou sur les diapos c'est que s'il vous dit : je suis sûr, ce serveur a qui vous parlez n'est pas sûr, je

ne peux pas vérifier donc débrouillez-vous. Donc il y a des caractéristiques qui sont mises en place pour faire des étapes différentes de sécurités.

Alors ce qu'un ISP devrait faire c'est de s'assurer qu'il n'y a pas de défaillance de validation lorsqu'il y a des attaques, ou lorsqu'il y a des problèmes sur l'internet, etc., etc.

[ALFIFA] : Je viens du Bangladesh. Je ne sais pas si ma question vous correspond, je ne sais pas si vous êtes la bonne personne pour y répondre. Mais en attendant, si vous avez fait face à des incidents importants par le passé, comment avez-vous fait pour entraver ces problèmes ?

WES HARDAKER: Oui, vous pouvez allez à l'atelier de travail du DNSSEC bientôt. On va parler bien sûr du roulement de la clef, etc. et on va vous expliquer comment on gère cela.

RUSS MUNDY : Je n'ai pas très bien compris la question, mais de toute façon, dans le cas du roulement de la clef KSK, nous avons vu qu'il n'y a pas eu de problème.

Il y a eu quelques différences au niveau du trafic, une fois que l'ancienne clef a été mise de côté.

Nous aurons une séance là-dessus et nous vous fournirons des informations sur le sujet.

Vraiment, au niveau opérationnel, il n'y a pas eu un impact important au niveau du roulement KSK. Ça a été un succès opérationnel et franchement, ça a été un grand succès.

WES HARDAKER: Oui, il y a des présentations que vous pouvez consulter sur l'internet, sur le web. Vous pouvez ainsi consulter la présentation sur le délai du roulement de la clef.

Il y a donc des données aussi qui ont été publiées depuis le dernier roulement de la clef. Venez me voir à la fin de la séance et je vous donnerai les liens pour que vous puissiez aller voir les présentations sur internet ou les vidéos.

Y a-t-il d'autres questions ? Il nous reste un peu de temps.

Très bien, je ne vois plus de main levée. Je vous remercie pour toutes vos questions, très intéressantes. Vraiment nous avons eu aujourd'hui un public très informé, les questions étaient vraiment techniques. Vous aviez fait vos devoirs avant de venir.

Si vous aviez d'autres questions, n'hésitez pas à me les poser plus tard.

Cette technologie, ça prend du temps. Nous ça fait 20 et quelques années qu'on gère. Donc de votre part, il n'y a pas de question idiote. Il y a beaucoup de choses à apprendre sur le sujet, n'hésitez pas.

Nous serons là, après cette séance, venez nous voir pour poser des questions. Sinon, passez une bonne soirée, profitez de la semaine à ICANN. Venez à nos séances de mercredi, nos séances sur le DNSSEC.

Je vous remercie.

Merci.

**[FIN DE LA TRANSCRIPTION]**