MARRAKECH – DNSSEC pour tous : guide du débutant
Dimanche 6 mars 2016 – 16h45 à 18h15 WET
ICANN55 | Marrakech, Maroc

JULIE HEDLUND: Bonjour à tous, je suis Julie, du personnel ICANN, nous allons commencer le DNSSEC pour Tous dans quelques minutes, je vous encourage donc à venir dans la salle et à vous asseoir, venez devant, venez près de nous et ensuite nous aurons du temps dédié aux questions/réponses, mais pour l'instant nous aimerions que vous veniez nous rejoindre, nous allons commencer très bientôt, bienvenue encore une fois à la session DNSSEC pour Tous : un guide du débutant.

Veuillez bien venir nous rejoindre, trouvez vos chaises, asseyez-vous, nous attendons que tout le monde soit là pour commencer, donc il s'agit de la réunion du DNSSEC pour Tous comme vous le voyez sur l'écran merci.

DAN YORK: Bon après-midi à tous, comment allez-vous ? Nouvel intervenant sur le panel, je m'appelle DAN YORK. Nous allons parler du DNSSEC pour Tous, je suis désolé pour le retard, nous pensions avoir la vidéo dans cette salle, mais nous allons faire un sketch en fait, et maintenant nous (inaudible) tous à distance que nous

allions avoir une vidéo, mais nous n'avons pas de vidéo, nous essayons de voir si nous pouvons faire autre chose pour avoir donc cette vidéo, ça n'a pas fonctionné, nous allons continuer et nous allons ainsi faire notre sketch. Nous avons de l'interprétation donc nous allons devoir tous parler lentement et moi je suis la première victime parce que vous ne voulez pas que je me mette à parler français, après avoir dit je m'appelle Dan, je suis un comptable, c'est tout ce que je peux dire, pamplemousse, je connais le mot pamplemousse. J'essaye.

Combien d'entre vous connaissent quelque chose du DNSSEC ? Ou de la sécurité DNSSEC ? Quelques personnes. Combien de personnes ont assigné un domaine avec le DNSSEC ? Combien d'entre vous ne savent ce que c'est un résolveur validé ? Donc si vous regardez l'ordre du jour, vous avez dû recevoir d'ailleurs un agenda, comme celui-là, si vous n'en avez pas, nous avons des feuilles avec cet agenda.

Dans cette réunion, je vais vous parler l'histoire de ce qu'aurais pu être le DNSSEC, donc expliquer ce qui rend le DNSSEC si important, si spéciale. Nous allons parler des concepts derrière le DNSSEC, utiliser des exemples, etc. Vous voyez qu'il y a des gens autour de nous qui ont déjà des T-shirts, cela va nous permettre de faire un sketch et de vous raconter une petite histoire. Je vais commencer, j'avais poussé le bouton dans le mauvais sens.

Bon, nous allons commencer par revenir en arrière, nous allons aller vers les origines du DNSSEC, 5000 ans JC, vous êtes prêts ? Voilà, ça, c'est Ugwina, elle vit dans une grotte sur le bord du grand Canyon, et voilà Og, il vit dans une grotte de l'autre côté du grand Canyon. Ils habitent loin l'un de l'autre, cela prendrait beaucoup de temps pour faire le tour, il faut qu'ils descendent et qu'ils remontent, donc ils ne se parlent pas souvent. Durant l'une de leurs visites, ils se sont rendu compte qu'il y avait de la fumée qui sortait de leur feu, cette fumée montait, donc ils ont eu cette idée : oh tiens, on pourrait commencer à utiliser des signaux de fumée et on pourrait parler d'un côté de l'autre du Canyon. On va communiquer un jour, le futé Kaminski déménage à côté de chez Og et puis il commence à envoyer aussi des signaux de fumée. Maintenant pour Ugwina, c'est la confusion, elle ne comprend pas qui envoie les signaux de fumée, elle ne sait pas quels signaux de fumée, l'information correcte, elle ne sait pas, elle est désorientée, donc elle décide de descendre dans le Canyon pour trouver la réponse. Et Ugwina et Og vont voir le sage du village qui s'appelle Diffie, mais il a une petite idée de ce qui pourrait être fait pour régler le problème, il va donc dans le fond de la cave de Og et dans cette grotte, il trouve une pile de sable bleu bizarre, c'est un sable que l'on ne trouve que dans la grotte de Og.

Donc il revient en courant et jette du sable bleu dans le feu, et la fumée devient ainsi bleue. Maintenant d'un seul coup Ugwina et Og peuvent se parler, communiquer d'un côté de l'autre du Canyon, parce qu'elle sait que la fumée bleue et celle qui l'intéresse. Donc tous les autres signaux de fumées ne sont pas intéressants pour elle, en fait, c'est ce que l'on fait avec le DNSSEC. On fournit un peu une fumée bleue spéciale, quelque chose d'unique que vous pouvez offrir en disant : voilà, ceci est l'information que j'ai besoin de donner. Personne n'a la couleur de ma fumée, la fumée de Marc peut être rouge celle Bob, verte, d'autre orange, chacun à sa couleur, mais vous avez donc une façon unique de faire les choses. DNSSEC vous fournit une façon de différencier les informations pour vous assurer que vous donniez une information précise.

Pour regarder cela avec plus de détails, à un très haut niveau, si vous avez vu ce genre de DNS, vous voyez la racine, vous avez les TLD différents et puis vous avez les domaines de second niveau. Voilà la structure telle qu'elle est. Chacun d'entre nous, lorsque nous allons sur un site web, quand nous envoyons des courriels, tout ce que nous faisons sur internet, nous utilisons un résolveur, résolveur DNS sur nos téléphones, sur nos ordinateurs, il y a donc des résolveurs qui utilisent des noms de domaines que ce soit google.com, nic.ma quelques soit ces noms de domaines, il change donc les noms de domaines en

adresse IP, il utilise cela pour communiquer c'est ce que le DNSSEC fait.

Chaque outil a un résolveur, le résolveur reçoit l'information en retour et la conserve pendant un certain moment, cela s'appelle un cache, cela donc conserve ou stocke ces données pendant une heure, une semaine, pendant une certaine période de temps, par exemple l'adresse IP d'icann.com, peut être telle ou telle adresse et elle va conserver les données. Le défi c'est que le DNS n'a pas de sécurité, Marc, par exemple peut venir et essayer de s'immiscer entre les deux et donner la mauvaise adresse IP à quelqu'un d'autre, on va le croire, car Marc est plus près, donc il peut dire à la personne à côté de lui avant que moi j'intervienne, quelle est la façon de faire telle ou telle chose, donc, voilà ce qui manque au DNS.

Les caches aussi peuvent être facilement empoisonnés, ce que cela veut dire si le résolveur de ce Monsieur reçoit l'information de Marc avant la mienne, il va utiliser cette information jusqu'à ce qu'elle soit expirée, nous en parlerons tout à l'heure, nous allons faire un petit sketch à ce sujet, je vais donc amener les acteurs du DNSSEC sur la scène, nous avons un groupe d'acteurs, nous avons donc une équipe qui se vête de leur T-shirt.

Je ne suis pas la personne qui raconte d'habitude, donc malgré tout, je vais vous présenter tout le monde, nous sommes un peu désorganisés. Ce qu'on va faire, c'est un petit sketch. Et vous ! vous voulez bien vous organiser ? Ça va aller ? Alors M. Wes qui va jouer le rôle de l'utilisateur final, Joe l'utilisateur, et puis vous avez Jacques Latour qui va être le ISP, nous avons Andrew, qui va faire le serveur racine au centre de l'action de DNS, Juan va être le serveur com et puis Russ va être le serveur banque.

Donc le DNS, est un distributeur de base de donnée massive, nous allons faire un petit sketch à ce sujet, ceux d'entre vous qui connaissent le DNS vous allez voir que nous allons prendre un peu de liberté sur le fonctionnement des choses. Nous voulons vous donner une idée générale de ce qui se passe. Nous allons utiliser quelques scénarios, nous allons tout d'abord utiliser la banque en ligne, Joe l'utilisateur veut aller faire quelque chose sur le site de sa banque, il veut aller sur www.bigbank.com. Voilà ce qui va se passer.

WES HARDAKER: Je veux aller payer ma facture d'électricité, donc amenez-moi à ma banque, amenez-moi à www.bigbank.com, je veux payer ma facture d'électricité je ne sais pas exactement où cela se trouve sur internet, donc je vais demander à l'ISP où ça se trouve.

JACQUES LATOUR: Je suis le serveur, je viens juste de me réveiller, je n'y connais rien, je ne sais pas ce qui se passe, donc il faut que j'aille voir où se trouve bigbank.com, je reviens vers vous avec une réponse tout à l'heure, tout ce que je sais c'est où se trouve la racine, donc je vais voir la racine, bonjour, je cherche www.bigbank.com, vous savez où c'est ? Alors le serveur racine répond et lui dit :

ANDREW: Ah, je ne sais pas où ça se trouve, mais je sais où est .com, je sais que c'est 1.1.1.1.

JACQUES LATOUR: Je vais aller sur 1.1.1.1. Bonjour .com vous savez où se trouve bigbank.com?

WARREN KUMARI: Je ne sais pas où c'est, mais je sais où c'est bigbank.com c'est à 2.2.2.2, vous devriez aller leur demander.

JACQUES LATOUR: Bonjour je cherche bigbank.com vous savez où c'est?

RUSS MUNDY: Oui en fait répond bigbank, en fait je sais où ça se trouve bigbank.com c'est à 2.2.2.3.

JACQUES LATOUR: Ah une réponse très bien. On revient vers l'utilisateur et je lui dis, voilà l'adresse est 2.2.2.3.

WES HARDAKER: Maintenant je vais pouvoir envoyer 1000 dollars à ma compagnie d'électricité.

DAN YORK: Cette communication entre Joe qui parle à son ISP, son résolveur, c'est une situation qui se passe souvent ou des milliers de fois, à chaque fois, qu'on ouvre une page web, à chaque fois qu'on communique avec qui que ce soit, quelle que soit les applications, tout ce qui doit nous donner une adresse IP. Quand on parle du vrai côté des choses, du côté cache, vous savez qu'à l'ISP, la racine a déjà les informations, ainsi l'ISP pourra retourner vers Joe rapidement et dire, ah oui sais où c'est puisque Joe l'utilisateur a déjà toutes ces informations dans son cache, mais ça ne va pas aider notre histoire, donc on évite de parler de cela.

Est-ce qu'on est prêt maintenant pour l'autre scénario ? Maintenant nous allons montrer ce qui se passerait avec le DNS régulier, sans le DNSSEC. C'est juste le DNS comme il serait le cas

aujourd'hui. Joe va recommencer seulement vous allez voir c'est quelque chose de différent cette fois-ci.

WES HARDAKER: Oh mon dieu! J'ai oublié de payer l'électricité! Donc je vais retourner à www.bigbank.com. Mais je me souviens où c'est. Est-ce que M. l'ISP, vous pouvez me dire où se trouve bigbank.com?

JACQUES LATOUR: Ah non, je viens de me réveiller, je ne connais pas l'information, mais je sais où se trouve la racine. Allo bonjour M. racine, je cherche bigbank.com vous savez où c'est ?

ANDREW: Je ne sais pas où ça se trouve, mais je sais où est .com. .Com est à 1.1.1.1.

JACQUES LATOUR: Merci boum boum boum je vais vers .com et je dis voilà, je cherche bigbank.com, vous savez où il se trouve ?

WARREN KUMARI: Je ne sais pas où c'est, mais je sais que bigbank.com est à 2.2.2.2.

JACQUES LATOUR: Non, je suis désolé, je continue à poser des questions, je ne suis pas très intéressant, pas très intelligent pardon, donc vous savez où ça se trouve ?

JAY DALEY: Oh oui, vous pouvez trouver cela à 6.6.6.6.

JACQUES LATOUR: C'est bien, merci beaucoup. Ah je reviens vers Joe. Joe, vous savez vote bigbank.com se trouve à 6.6.6.6.

WES HARDAKER: Oh merci ! Ma facture d'électricité est très élevée ce mois-ci. Je dois 1 million de dollars, mais je suppose que je dois payer.

DAN YORK: On les applaudit!

Comme vous avez vu, ce qui s'est passé c'est que Jay qui jouait le diable, c'est l'homme au milieu, il a donné la mauvaise réponse à Ross. En fait, il a été plus rapide que bigbank.com. Il est arrivé plus rapidement, donc il a donné la mauvaise information. Il a poussé Russ et il a donné sa propre information. Jay est arrivé et il a donné donc cette information avant lui,

donc, c'est l'attaque fondamentale que nous essayons de prévenir avec le DNESSEC, nous essayons de prévenir les gens pour qu'ils n'obtiennent pas la mauvaise information. Et ça c'était même avant que l'utilisateur soit connecté sur le site, il n'était même pas arrivé à igbank.com. On essaye de s'assurer que Joe arrive sur le bon site, c'est ça qu'on essaie de faire.

Donc maintenant ... par contre je parlais, ils ont déjà commencé à continuer le sketch.

Donc pour faire la sécurité, pour assurer la sécurité, nous savons qu'il y a deux parties, il y a la partie de signature, pour les opérateurs de zone qui doivent mettre une signature cryptée, ils doivent signer leur zone, cela veut dire que cela prend un logiciel qui génère une signature qui à la base explique que l'information est jute, exacte.

Par exemple si vous pensez à vos médicaments qui sont enveloppés et qui sont scellés, vous ne pouvez pas ouvrir les boîtes de médicaments, parce qu'ils sont dangereux, et cela est mis en place par l'usine (inaudible) la manufacture de ces médicaments, on ne peut pas les ouvrir parce qu'ils sont dangereux, c'est exactement ce que l'on fait, on essaye de protéger l'information dès le départ. Donc ils vont signer et ils vont faire passer l'information entre bigbank jusqu'au TLD, et

ensuite le TLD va passer l'information à la racine, donc il crée une chaîne de confiance.

Donc un attaquant, disons, ne peut pas prétendre à une signature, ne peux pas s'immiscer (inaudible) côté, vous voyez notre ISP ici, doit vérifier cette signature parce que si de ce côté-là ils ont signés c'est très bien, mais s'il ne vérifie pas cette signature, ça ne sert à rien, il n'y a pas de sécurité ajoutée. Donc il va valider la validation du DNSSEC, il va valider la signature, il va s'assurer que ces informations sont correctes.

Dans notre prochain sketch, l'acte 3, en fait l'acte 3 est déjà passé avec la signature et tout ça, c'est fait, nous allons passer à l'acte 4. Nous allons voir comment cela va se passer avec le DNSSEC.

WES HARDAKER: (inaudible) utilisateur, je vais envoyer à Dan, de l'argent, donc je vais aller à bigbank.com, et je vais transférer de l'argent à mon ami. Donc je vais passer l'information à mon ISP, qui a un résolveur validé.

JACQUES LATOUR: Bon, vous avez pris une bonne décision, vous voulez aller à bigbank.com?

JACQUES HARDAKER: Voilà je suis l'ISP, je me réveille, je n'y connais rien, je vais demander à la racine s'il sait où se trouve bigbank.com.

ANDREW: Je suis le serveur Racine, voilà je ne sais pas où se trouve bigbank.com, je sais où se trouve .com. C'est à 1.1.1.1. Et puis je vais signer l'information par contre, valider avec ma signature. Voilà c'est fait.

JACQUES LATOUR: Ah, mais c'est très bien la signature elle correspond elle est validée c'est bon, maintenant je vais voir .com. Bonjour .com, je veux aller à www.bigbank.com, vous savez où se trouve bigbank.com ?

WARREN KUMARI: Oui je sais où ça se trouve, c'est à 2.2.2.2. Voilà ma signature de vérification allez-y !

JACQUES LATOUR: Ah, je vais vérifier votre signature, c'est bon maintenant je vais à bigbank.com. Bonjour M. BigBank.com, je veux aller à bigbank.com.Ah intervient le diable.

RUSS MUNDY: C'est à 6.6.6.6.

JACQUES LATOUR: Merci beaucoup. Merci, je vais vérifier votre signature. Ah non ce n'est pas bon ! Partez ! Laissez-nous tranquilles ! Vous croyez ça un peu ?

(inaudible) bigbank.com team. Merci M.ISP, je sais où se trouve bigbank.com. Et c'est à 2.2.2.3. Et voilà, je vais signer la validité avec ma signature.

ISP répond Merci!

JACQUES LATOUR: Je vais vote signature, si cela correspond. Alors Joe l'utilisateur, l'adresse IP est 2.2.2.3.

WES HARDAKER: Ah! Bon. Je peux envoyer de l'argent à mon ami.

DAN YORK: Très bien, tout cela est très bien, on les applaudit.

Maintenant, une question pour vous : qu'est-ce qu'à du faire Joe l'utilisateur dans ce scénario ? A-t-il du faire quelque chose ?

Non, cela a fonctionné pour lui derrière les coulisses si vous voulez. Qu'a fait l'ISP ? Il a validé, il a vérifié la signature. Et toutes les autres choses se sont passées entre les serveurs. En fait, à un niveau très simple, c'est ce qui se passe au niveau du DNESSEC, c'est ce que nous essayons de faire, nous essayons de prévenir le diable de rentrer, de s'immiscer dans la conversation.

Nous allons parler un peu de toutes ces étapes, mais voilà donc le processus fondamental de base. Vous comprenez, c'est bon ?

On va faire donc une révision d'un couple de chose, d'autre chose, on a fait ça, on a fait ça, on a fait ça, et ça et on en est là.

Deux ou trois choses dont on a parlé, on a parlé de signature numérique et on a parlé de clé, avoir des clés qui correspondent à vos informations. Donc quand vous publiez vos informations dans le DNS, comme vous l'avez toujours fait, vous publiez aussi une signature. Vous générez cela, et le logiciel existe pour faire cela. Vous pouvez publier toutes ces informations qui sont conservées dans le DNS.

Excusez-moi il y a une pièce qu'on a oubliée. Quand le résolveur va vers la racine, et demande une vérification des signatures, le résolveur connaissait déjà la clé de la racine, il connaissait cette clé qui était derrière cela. Une chose dont vous allez entendre parler dans le monde de DNESSEC, c'est cette discussion de retour de clé, il faut changer la clé, on en parlera plus mercredi durant notre atelier technique. C'est ce qui donc permet les bonnes informations d'être transférées. Quand on sait qu'il y a une mauvaise information, qu'il y a une rejection, un rejet, disons, ce qui se passe c''est que l'ISP fait une autre demande et trouve le bon serveur et reçoit la bonne information.

On a fait cela et donc, je vais passer le micro à Russ pour qu'il nous fasse le détail un peu plus technique et ensuite nous reviendrons vers vous pour des questions/réponses. Et nous avons beaucoup de gens ici qui peuvent nous aider si vous avez des questions.

RUSS MUNDY: Très bien, maintenant je ne suis plus bigbank.com, comme vous le voyez, je suis Russ Mundy, je suis là pour vous aider avec plus d'informations sur toutes les parties techniques du DNESSEC. Pourquoi devons-nous nous préoccuper du DNESSEC ? Comme on l'a fait souvent, il y a

comme vous le savez de plus en plus d'attaques et c'est ce qui rend le DNESSEC si important, parce que chacune des applications telles quelle soit, sur l'internet, car il y a très peu d'exceptions, il y a très peu de personnes qui utilisent encore des adresses IP, mais bon on utilise le DNS pour tout faire sur l'internet maintenant, donc quelqu'un veut attaquer une application, où va-t-il commencer ? Il va commencer au sein de l'application et aussi dans le DNS lui-même, en changeant les informations du DNS.

Que fait le DNS ? Au niveau fondamental, cela change les noms qu'on aime utiliser en numéro et en changeant l'infrastructure pour faire changer les données d'un point à un autre. Donc on va à un bon endroit ou dans un mauvais endroit. Et vous en tant qu'utilisateur, vous n'avez aucune façon de savoir ce qui se passe et c'est vraiment un problème très sérieux. Et c'est donc la menace d'usurpation dont on parlait. Lorsqu'il y a des attaques d'usurpations, l'utilisateur qui demande une information obtient une mauvaise information et ce qui se passe après, peut être visible par l'utilisateur ou pas, mais l'intention de l'attaque et surtout pour faire quelque chose de mauvais, menacer un utilisateur ou un serveur, il y a des outils disponibles pour usurper le DNS ?

Oui il y en a, je ne vais pas vous les montrer sur des diapositifs, cela rendrait les choses trop faciles, je ne veux pas faire de

publicités sur ces outils bien sûr, mais l'information est sur internet bien sûr et il y a un professeur qui donne un cours là-dessus d'ailleurs, c'est un cours d'informatique qui permettait de construire un logiciel pour attaquer le DNS. Ils utilisaient cela pour enseigner au niveau universitaire, et il n'y avait aucune éthique associée avec cela, c'était juste un exercice de programmation de logiciel, donc l'information est là, et elle est facile à trouver.

Qu'est-ce qu'on essaie de faire avec le DNESSEC ? On essaie de protéger l'utilisateur pour qu'il obtienne une information correcte, et ensuite l'utilisateur peut aller à l'endroit où il veut aller sur internet. Voilà un diapositif qui donne une illustration de ce que montrait le sketch que vous avez vu, c'est un peu abrégé parce que je n'ai pas utilisé toutes les flèches que j'aurais pu utiliser. Cela passe d'un utilisateur à par exemple bigbank.com, la demande va vers un serveur de nom et ensuite revient avec la réponse. Donc quand on compte toutes les demandes d'un point à un autre, vous savez qu'il y a quatre paquets d'échange qui doivent se passer avant que l'utilisateur soit en fait connecté avec le serveur de web.

Toutes ces choses se passent dans les coulisses, ces choses-là se passent très vite, elles sont très rapides, nous avons ici une photo d'un site web qui est là pour montrer à l'utilisateur si le DNESSEC fonctionne de bonne manière ou s'il ne fonctionne pas

bien. Une des choses que nous avons fait ici, nous avons un exemple spécifique, encore une fois, une autre illustration, un autre graphique avec le diable que vous voyez dans le cercle jaune en bas qui donne la mauvaise réponse, etc., et celle de droit où vous voyez le diable qui envoie les gens vers le mauvais site.

Dans ce cas là vous avez un exemple, voilà ici des photos de site que j'ai pris d'un vrai usurpateur pour vous montrer, pour illustrer un peu mon exemple. Alors, nous avions utilisé un site et quand on utilisait le DNESSEC pour aller sur le site, on obtenait le contenu correct du site, mais avec un usurpateur, on obtenait juste une portion de cette page, pas tout le site en entier, mais seulement une portion de la page.

Comme vous le voyez à gauche, le site qui a la vérification du DNESSEC, vous voyez le contenu du site est sur la page de droite, vous voyez il y a une histoire qui est fausse. Vous voyez qu'il s'agit d'une usurpation, c'est juste pour illustrer le point. Donc il peut usurper tout le site en entier, ou seulement une petite portion du site, l'utilisateur va obtenir la mauvaise information. Tout cela dépend de comment l'usurpateur va travailler.

Cette image ressemble à une illustration par exemple, lorsque vous remplissez un formulaire avec plusieurs niveaux, ici vous

avez une image qui a été produite il y a 8 ou 9 ans, on l'a vérifié plus récemment, c'est plus dense encore, donc voilà toutes les étapes par lesquelles il faut passer pour remplir les navigateurs pour le site web du DNS. Plus de 100 beaucoup plus de 100. Jusqu'à quelques années c'était 70 maintenant c'est plus de 100.

Donc on peut penser de manière générale un site web, et on pense que c'est simple, mais cela ne l'est pas, les sites web commerciaux sont très lents et ont beaucoup d'applications en terme de DNS. Donc chacun a à faire avec ce type de menace.Donc l'importance de tout cela est de tout ce qui concerne la protection du contenu du DNS à avoir avec le DNS lui-même, le DNS est critique pour que les utilisateurs soient assurés qu'ils obtiennent le contenu correct, mais ça n'est pas plus important que le contenu lui-même, car ce qui est véritablement important c'est le contenu, le DNESSEC existe pour s'assurer que le contenu puisse être déterminé par toutes ces étapes, donc toutes ces étapes sont aussi importantes que le contenu, certaines personnes n'ont pas les idées très claires par rapport à cela.

Voilà quelques exemples rapides de mis en oeuvre, d'abord le déploiement standard s'agissant du contenu également du serveur faisant autorité, du serveur récursif, il s'agit du fournisseur de service internet, qui fait le tour et qui pose des

questions, qui fait des demandes aux questions de l'utilisateur Joe.

Donc c'est la manière dont le contenu est ajouté et sorti. Alors ce qu'ajoute le DNESSEC c'est un certain nombre d'étapes supplémentaires pour s'assurer que vos obtenez la mise en place du DNS et que ce contenu et contrôlé et vérifié. Ce qu'on fait ici, c'est de parler du niveau de facilité ou de difficulté pour que le contenu soit vérifié ou si vous êtes un utilisateur d'une grande entreprise, qu'on inclut le DNS quels sont le type de choses qu'il faut faire pour s'assurer de cela. Je ne vais pas rentrer dans les détails de tout cela, car on veut garder du temps pour que vous puissiez poser vos questions à la fin de cette séance.

Donc voilà le principal message que j'aimerais vous transmettre, tous les éléments qui concernent le DNS et la sécurité du DNS, ça avoir avec le contenu des données de zone, c'est le contenu qui fait la différence, parce qu'il faut l'introduire de la bonne manière, il faut le gérer de la bonne manière, il faut le protéger de la bonne manière, avec le DNESSEC.

Donc dans le cas d'espèce ce sont les mêmes étapes, il s'agit des données signées et le serveur récursif fait la validation. Donc il s'agit d'une mise en oeuvre de ces deux aspects essentiels. Ces informations sont validées lorsque les données ressortent, donc

c'est une manière simple, de mettre en oeuvre le DNESSEC. Donc en terme de ce peut faire les utilisateurs par rapport à la mise en oeuvre au sein de l'organisation, quelle qu'elle soit, qu'il s'agisse d'activité commerciale qui reposent essentiellement sur le DNS, il est fort probable que vous ayez une équipe DNS déjà bien achalandé.

Ensuite, cette équipe peut mettre en oeuvre le DNESSEC elle-même, en général, c'est ce qu'elles font. Si vous appartenez à une opportunité qui sous-traite ce genre d'activité, alors il faut demander ces équipes de sous-traitances, et leur demander de mettre en oeuvre le DNESSEC dans le cadre des activités DNS qu'ils effectuent pour vous.

Et si ce n'est pas le cas, je vous recommande vivement d'envisager de sous-traiter, car c'est quelque chose de très important, demander à vos fournisseurs si vous le faites vous même ou demandez à vos fournisseurs de service internet de le faire pour vous, demandez un soutien DNESSEC, c'est probablement le message le plus important.

Est-ce que vous avez le DNESSEC ? Et si ce n'est pas le cas quand est-ce que vous allez l'acquérir parce que je le veux et je le veux maintenant!

Je suis à votre disposition si vous avez des questions, on a des experts qui sont également à votre disposition pour répondre à vos questions.

DAN YORK: Merci, je crois qu'on a 1/2 heure, on a beaucoup de temps, j'aimerais écouter vos questions dans la salle, je vous écoute. Allez je vais marcher un petit peu pour aller vous rejoindre.

INTERVENANT INCONNU : Je m'appelle Déris de l'Uganda, j'ai une question sur la sécurité. Je me demande, l'une des manières de s'assurer qu'il y a une sécurité du certificat SSL, et comment est-ce qu'on peut s'assurer du certificat SSL ?

DAN YORK: Je vais y répondre d'ailleurs, c'est une excellente question, parce qu'on peut poser la question, j'ai un DNS, j'ai un SSL, donc je suis protégé, je n'ai pas de problème, or il y a plusieurs choses qui peuvent se produire.

D'abord vous voyez ici que l'un des domaines d'expositions c'est justement celui-là, c'est de vous rendre sur une adresse IP erronée. Donc menace d'usurpation. Et le DNESSEC peut vous protéger de cette menace spécifique, mais là vous passez à un

autre niveau, à des questions qui touchent au type de certificat utilisé, est-ce que j'utilise le bon certificat et au sein du DNESSEC on a quelque chose qui s'appelle le protocole DANE, il s'agit d'un certificat qui passe par le DNS, qui est signé et vérifié par le DNESSEC, et donc on peut savoir grâce à la signature cryptographique, que c'est validé, c'est correct et l'utilise par exemple pour les courriers et les autres.

Donc pourquoi ce site web est usurpé ? Ça implique beaucoup d'autres questions qui se produisent à un plus haut niveau, il s'agit des applications très souvent leurs sites web ont des problèmes en terme de forme qui permettent aux gens de les usurper ou bien on peut rentrer sur les serveurs sans le DLS, car le DNS protège la communication entre le serveur et le navigateur, donc on protège les données là, mais le DLS protège les données ailleurs, mais le DNS ne vous protège pas un l'autre niveau parce que c'est une communication finalement entre le serveur et le navigateur, mais il y a d'autres manières d'usurper.

RUSS MUNDY: Alors si vous regardez ici les flèches rouges, vous voyez les demandes du serveur et en vert les demandes http/https, et ce que fait le DNESSEC, c'est de garantir que vous allez faire le bon serveur web. Si le serveur web lui-même a été attaqué, ou a reçu

une menace, c'est quelque chose que le DNESSEC ne va pas pouvoir résoudre.

Ou si le certificat DNS a été menacé ou que quelqu'un a fait quelque chose, car il a menacé cette sécurité, alors le DNESSEC peut intervenir, et à chaque fois que vous allez sur un site où il y a des fonctionnalités d'applications, alors ce site doit fonctionner correctement et le DNESSEC s'assure que vous allez sur le bon site, mais pas que ce site fonctionne de la bonne manière.

INTERVENANT INCONNU : Donc la sécurité n'est pas garantie ?

DAN YORK: Non le DNESSEC vous garantit que allez sur la bonne adresse IP, que vous obtenez une connexion cryptée entre les serveurs, mais ce qui se passe en fait, pour le serveur c'est qu'on est tous sur le navigateur web, vous travaillez sur votre ordinateur portable ou autre ça, ça va avec la communication. Le DNESSEC garantit les adresses IP, mais ça ne couvre pas tout, il y a toute une série de problèmes qui se pose pour les navigateurs web.

Alors, comment se déplacer dans cette salle plus vite ? Peut-être des rollers.

INTERVENANT INCONNU : D'après les diagrammes à l'écran, il semblerait que le DNESSEC doit être mis en oeuvre par différentes parties, donc mis en oeuvre par les FSI qui doivent les soutenir, les opérateurs de registre et chaque site web doit le soutenir.

DAN YORK: En fait chacun des noms de domaines. Oui effectivement, mais il y a deux aspects, l'aspect validation, vérification que les FSI fournisseurs service internet, font, et ça, c'est relativement facile à faire, vous pouvez relier ce genre de chose ou vous pouvez vous adresser à vos fournisseurs, mais il faut que vous soyez conscient que s'il y a un problème de signature, vous pouvez prévenir les autres. Attention, n'allez pas sur ce site, donc vous pouvez les prévenir si vous rencontrez des problèmes; ça, c'est pour ce qui concerne la validation.

Pour ce qui concerne les signatures, oui ça, ça implique la racine signée en 2010 et la plupart des TLD génériques et des nouveaux TLD génériques ont tous été signé au premier niveau. Beaucoup des extensions génériques GTLD ont été signées, même si l'Afrique n'a pas encore signé ces GTLD et on a travaillé avec certains d'entre eux. Il faut que vos bureaux d'enregistrement soient soutenus parce qu'il faut qu'il y ait cette signature, donc il

y a d'un côté la validation qui est simple et celui de la signature où il faut qu'il y ait ces 3 acteurs qui participent.

Julie vous voulez intervenir ?

JULIE HEDLUND: Oui j'aimerais rappeler aux gens s'il vous plait lorsque vous posez une question, présentez-vous s'il vous plait au micro.

Oui par rapport à la validation des FSI, environ 20% des demandes de DNS passe par le résolveur, donc ce n'est pas un chiffre aussi bon que celui qu'on escompterait, mais bon c'est un bon pourcentage.

DAN YORK: Oui on le fait par défaut, donc pour ceux qui utilisent les adresses IPv6 tout cela est validé par défaut.

STEVE: Oui, je suis d'Amazone.

DAN YORK: Vous en tant que titulaire de nom de domaine, vous n'avez pas forcément grand-chose à faire, mais ensuite le DNS qui héberge l'opérateur lui a quelque chose à faire. Donc très souvent c'est également le bureau d'enregistrement, mais pas forcément par

exemple, vous vous êtes opérateur DNS donc vous servez toutes ces zones, il faut trouver les zones parce qu'à chaque fois, qu'il y a des changements, il faut y avoir de nouvelles signatures.

Mais l'importance c'est que les opérateurs doivent signer et les bureaux d'enregistrement doivent tenir ces informations pour les transmettre aux opérateurs de registre et l'important c'est que les bureaux d'enregistrement qui ne soutiennent pas ou qui ne permettent pas d'avoir des enregistrements, ce n'est pas une bonne chose, donc il faut passer à un autre bureau d'enregistrement. Mais Jacques voulait intervenir.

JACQUES LATOUR: Vous avez dit que vous travaillez pour Amazone, bon alors je pense que certains grands opérateurs, peuvent signer leur propre zone DNS et ce qu'on fait maintenant c'est d'essayer de mettre en place une nouvelle interface pour les opérateurs puissent signer eux-mêmes les domaines sans passer par les bureaux d'enregistrement. Ce problème de signature du DNS c'est votre responsabilité.

RUSS MUNDY: Oui merci de cette question, j'aimerais également ajouter que de fait le titulaire du nom qu'il opère ou pas les services associés au

DNS, c'est celui qui prend la décision. Moi je veux que le nom du DNESSEC soit signé, quelles que soient les opérations en jeu.

Nombre d'entre nous aimeraient vous donner beaucoup plus de détails, sur les questions que vous posez après cette séance, pour résoudre ce genre de problème opérationnel, et je pense que le principal défi, c'est de faire rentrer ça dans le système DNS. Merci

DAN YORK: Alors si vous n'avez pas encore saisi le message, sachez on peut être beaucoup plus pointu encore dans nos réponses. Y a-t-il d'autres questions dans la salle ?

ADEEL SADIQ: Du Pakistan. J'ai deux questions en fait, lorsque la banque transférerait ces informations à l'utilisateur Joe, c'est ma première question, ensuite est-ce que le diable peut utiliser ces informations lui-même avant même que la banque ait commencé ce processus.

DAN YORK: Est-ce que l'un des membres du panel veut répondre à cela ?

WES HARDAKER: Alors moi je suis Joe, alors je ne peux pas répondre à cette question, mais en tout cas, écouter, je vais prendre les choses par ordre.

D'abord il y a un problème entre l'utilisateur Joe et son fournisseur de service internet, la solution à cela c'est valider un résolveur, moi j'en ai un sur mon ordinateur portable, et je sais qu'on peut en mettre aussi sur les portables, ce n'est pas difficile, ce n'est pas sorcier, il y a d'autres étapes qu'il faut suivre, il y a un programme qui s'appelle DNSTrigger qui automatiquement peut l'activer si vous êtes dans un hôtel, ça ne fonctionne pas toujours, malheureusement ça se produit, donc il y a des solutions pour ce genre de chose, maintenant je cale un petit peu sur la 2e partie de votre question parce que je ne m'en souviens plus trop.

Oui quel était le problème entre bigbank et l'utilisateur ? Alors si vous vous souvenez dans la petite scène qu'on a jouait tous les acteurs échangeaient une signature auparavant, donc ils se sont mis d'accord avant. Donc, lorsque vous vous connectez à votre bureau d'enregistrement, vous demandez un nouveau domaine.com, alors vous pouvez dire à votre bureau d'enregistrement que vous avez besoin d'authentifier les données et qu'on ne peut pas insérer quelque chose n'importe où, donc on peut prévenir ce d'attaque de menace.

Donc, ce genre de menace aurait pu être prévenu.

DAN YORK: Jacques tu veux répondre ? Non c'est bon ça a été fait. Oui, parce que le diable aurait pu intervenir dans le paquet signé, ça aurait pu être possible, mais c'est une chaîne de confiance entre la racine et le TLD qui garantisse que même si le diable vient avec cette signature, le FSI (Fournisseur Service Internet) peut dire oui vous avez une signature, mais ça n'est pas la bonne signature, et donc ça le renvoie jusqu'à la racine. Donc le diable aurait pu intervenir entre l'utilisateur et les autres, mais nous avons un groupe de travail qui s'appelle Deprive, d'ailleurs on a le président de ce groupe de travail qui se penche sur la manière de rendre cette communication entre l'utilisateur et le DNS pour garantir une communication sûre entre le fournisseur de service internet et l'utilisateur.

Donc, l'une des manières c'est par exemple que l'utilisateur assure cette vérification lui-même.

HIBA ELTIGANI: Par rapport à ce processus de signature et la validation, il s'agit d'un certificat qui ...moi j'avais une question sur le certificat et la validation.

DAN YORK: Oui bien sûr, je vais vous donner plus de détails.

WES HARDAKER: Donc lorsque vous signez une zone, il faut stocker des clés sur votre machine, et il y a tout un document qui concerne les meilleures façons de le faire. Je ne me souviens plus de la référence de document, mais il existe. Donc il faut stocker le certificat et les clés et ce que vous introduisez dans le DNS, c'est quelque chose de public, donc vous faites un lien entre cette clé publique et le DNS, la clé privée vous la gardez sur votre machine ou de préférence sur un autre ordinateur, et le DNS a été conçu d'une certaine manière que vos clés privées soient stockées dans un endroit très spécial et que vous ne les sortiez que dans un certain cas.

Donc certaines personnes conservent leur clé privée en ligne pour qu'elles soient rapidement mise à jour parce qu'ils les changent très souvent, mais ça n'est pas nécessaire.

DAN YORK: Oui il y a ce qu'on appelle le document DPS, qui est disponible pour tous les TLD, et qui explique ce qu'ils font. La zone racine a un processus très strict pour protéger les clés privées et pour, mais ça rentre dans d'autres détails que je ne vais pas parler ici, mais les TLD utilisent d'autres mécanismes pour les domaines

individuels et tout ça, ça dépend du niveau de risque que vous voulez prévenir, donc à l'intérieur de votre logiciel et du serveur que vous utilisez, le résolveur DNS va fonctionner de telle ou telle manière.

En fait dans un fichier de (inaudible) on va vous dire : voilà, il faut faire appel à ce résolveur, et le DNESSEC va intervenir, mais, c'est très facile de retirer la partie commentaire et ça disparait, parfois il y a eu une autre étape supplémentaire, et il commence à faire cette validation pour tout le système DNS.

RUSS MUNDY: Alors j'aimerais aussi souligner que beaucoup de gens se penchent sur ce qu'ils considèrent être les principales fonctionnalités du DNS qui sont associés à leurs propres opérations du DNS, donc, la racine a tout une structure sécurité qui est très importante, il s'agit de modèle de sécurité, beaucoup de TLD utilisent aussi des modèles de sécurité, donc la seule manière de resigner une zone, et il s'agit du niveau le plus élevé de resignature, c'est de passer par une procédure très longue et donc c'est un travail très lourd. D'autres gens disent : voilà, ce contenu en fait n'est pas sensible, et l'entreprise pour laquelle je travaille sous-traite finalement, et ils ont déjà mis en place la procédure donc chaque activité individuelle doit voir

dans quelle mesure leur DNS est sensible à ce genre de chose ou pas.

Donc ça, ça dépend de votre gestion des clés, mais il faut le voir au cas par cas, pour chacune des activités, mais il y a beaucoup d'aide disponible, pour la plupart gratuite, parce qu'il y a beaucoup d'informations qui ont été publiées, beaucoup de ressources disponibles et d'informations disponibles qui peuvent vous aider à prendre des décisions parce que souvenez-vous qu'il s'agit surtout du contenu et de l'utilisation qui va être faite du contenu.

DAN YORK: Oui moi je dirais, en tant qu'utilisateur individuel, ah! excusez-moi, Jacques voulait intervenir.

JACQUES LATOUR: Oui pour les logiciels commerciaux, cliquez sur oui et en général, vous allez bien faire.

DAN YORK: Pour certains de mes domaines les opérateurs DNS que j'utilise, font que je vérifie une case et ils s'occupent de tout et pour un autre, je dois aller dans d'autre section pour voir ce que fait le DNS et je clic là-dessus pour dire voilà il faut que ça soit le DNS

qui le fasse et c'est tout ce que j'ai à faire. Et ensuite eux s'occupent de changer les clés pour moi, et ils le font de manière automatique.

Alors j'ai parlé de validation et mon ami Paul qui se trouve ici m'a dit que les nouvelles versions reliées ou non reliées sont des validations DNESSEC.

WARREN KUMARI: Oui, il y a aussi des fournisseurs DNS qui très prochainement vont faire le DNESSEC pour tous, donc ne vous inquiétez pas, ça va arriver.

DAN YORK: Oui, il y a également un atelier DNESSEC de 9h à 15h30, ça figure dans l'ordre du jour, dans le programme de la semaine, sur la signature du DNS et tous ces aspects très intéressants du DNS. On va parler également du travail de l'équipe qui signe ces noms à haut niveau.

INTERVENANT INCONNU : Bonjour, alors on parle des clés, est-ce que ces clés ont une date d'expiration ? Quelle est la durée de validité des clés ? Et que se passe-t-il lorsqu'elles expirent ?

DAN YORK: Je vais d'abord répondre à la deuxième question, donc si vous pensez au fait qu'il y a des signatures de vérification et que la signature cesse d'être valide, que pensez-vous qu'il va se produire ? Le résolveur de validation on va dire, ce n'est pas bon, ce n'est pas exact, vous ne pouvez pas atteindre votre destination.

Je vais vous raconter une petite histoire, il y a 1 an 1/2 si je me souviens bien, la NASA aux États-Unis, nasa.gov, l'agence spatiale, avait signé leur domaine, et tout ce passait bien. Comcast c'est un opérateur très important aux États Unis à démarré la validation de la DNESSEC pour de nombreux clients aux États Unis, la validation était bonne pour tout le monde. Tous ces gens avaient la validation DNESSEC,tout se passait bien. Et les gens de la NASA, ont fait une petite erreur, quelqu'un n'a pas fait très attention sur la date d'expiration. Typiquement pour une clé,on fait les choses pour une année, il y a des processus un peu compliqués, il y a des clés pour signer la zone et ainsi de suite, mais la grande clé dont vous devez vous préoccuper elle est là pour un an.

Donc à la NASA, quelqu'un n'a pas fait attention, il n'a pas fait son travail, et la clé a expirée, donc d'un seuls tous les gens qui étaient sur le réseau Comcast et c'était même avant Google, ça serait pire aujourd'hui d'ailleurs, tous les gens qui étaient sur le réseau Comcast ne pouvaient pas rentrer sur le site de la NASA,

ne pouvaient rien voir, pas de photos de l'espace, rien du tout, le problème bien sûr était que tous les gens pouvaient sortir leur téléphone portable, et regarder dessus, et comme le réseau ne faisait pas la validation DNESSEC, il ne pouvait pas aller sur le site. D'un seul coup, il y avait un autre facteur en fait, ça, c'est passé le jour où vous vous rappelez, il y a eu un blackout à travers le web, à cause du problème de législation qu'il y avait aux Etats Unis avec des problèmes, avec le gouvernement, avec le Congrés des Etats Unis, ce jour-là, il y a beaucoup de site qui se sont fermé en guise de contestation pour le gouvernement américain. C'était ce jour-là que les choses se sont passées.

D'un seul coup, avec Comcast, il y avait des gens qui pouvaient aller sur le site de la NASA sur leur portable, et d'autres gens sur leurs ordinateurs ne pouvaient pas aller sur le site et donc, les gens disaient : Comcast doit être en train de bloquer la NASA, il y avait des tas de conflits tout le monde disait : oh mon dieu que se passe-t-il ? Qu'est-ce qui se passe ? Ça a été résolu bien sûr et Comcast depuis ce jour-là a mis des mesures en place, et les gens de la NASA ont été excellents; ils ont bien travaillé avec Comcast pour documenter ce qui s'était passé.

D'ailleurs, je me souviens, ils ont fait une présentation durant l'un de nos ateliers il y a quelque temps. En fait c'était il y a un peu plus de 1 an 1/2, ça s'est passé il y a plus de 3 ans, j'avais oublié, donc la réponse à votre question c'est si vous ne faites

pas les choses de la bonne manière, cela peut créer un gros problème. La bonne nouvelle c'est qu'il y a des systèmes qui sont en place qui est automatisée et qui prévoit ce problème.

Est-ce qu'il y a des gens du Kenya ici ? Il y a quelqu'un du Kenya ? Il y avait un problème au Kenya il n'y a pas très longtemps, il y a 1 an je crois. Oui, en 2014, l'année dernière, peu importe. Il y a quelque temps le Kenya a eu un problème avec cela aussi, il y a eu une date d'expiration sur le TLD sur le .ke, d'un seul coup la chaîne de confiance c'est cassé parce que le TLD, d'un seul coup avait une mauvaise signature, donc tous les gens qui étaient signés sous cette ombrelle disaient bon tout va bien, mais quand le résolveur a voulu remonter la chaine, ils sont arrivés à .ke et .ke ne fonctionnait pas et donc la chaîne confiance ne fonctionnait plus.

Donc les chaînes ne fonctionnaient plus, donc vous voulez vous assurer de savoir quand la clé expire, donc signer, ce n'est pas seulement faire une chose, il faut faire attention à tout ce qui est inclut, faut faire très attention en tant que consommateurs.

Moi en tant que consommateurs je vais voir mon nom de domaine et tout ce que j'ai à faire c'est de cliquer sur la petite case, c'est tout, je n'ai pas à m'assurer de tout cela. Cela est fait pour moi. L'automation et les outils, il y a plein de nouvelles

choses, il y a des outils sur le DNS qui existent, il y a beaucoup de choses qui existent maintenant.

Je pense qu'il nous reste du temps pou une question peut-être, il nous reste 15 minutes, c'est très bien, y a-t-il d'autres questions ? Oui, là-bas!

MADAME (INAUDIBLE): Uganda. Qui se préoccupe de ces signatures ? Qui est responsable de ces signatures ? est-ce le propriétaire du nom de domaine, le serveur, qui ?

DAN YORK : Oui, c'est la personne qui fournit le service DNS. Donc le titulaire du nom de domaine, quelqu'un lui fournit l'information, Russ comme (inaudible) dans la photo qui faisait le bigbank, c'est lui qui fournissait l'information pour bigbank, c'est lui qui avait les signatures; vous , vous êtes le titulaire, vous vous êtes arrangés avec lui pour qu'il le fasse, vous allez peut-être le faire vous-même, le monsieur là-bas d'Amazone, il a son propre serveur, il gère son propre serveur, donc il fait tout ça lui-même, votre équipe technique si elle peut le faire elle-même, ils peuvent; mais c'est donc la personne qui opère le serveur.

Y a-t-il d'autres questions ? Il nous reste encore du temps. On peut avoir des questions en français si vous avez des questions

en français, Jacques va les traduire pour nous. Il n'y a pas de problèmes. Allez envoyer !

WARREN KUMARI: Oui, posez une question en Français ça serait sympa d'entendre Jacques répondre.

DAN YORK: Son français n'est put-être pas le même que le vôtre.

INTERVENANT INCONNU: Puisque vous avez convenu la signature c'est pour la résolution, est dans la suite de sa question, je ne comprends pas pourquoi quel est le rôle joué ici par le registrer ? Donc j'aimerais qu'on réponde juste pour le registrer pour indiquer un peu le processus de signature.

JACQUES LATOUR: Donc quel est le rôle principal du registrer ?

INTERVENANT INCONNU: Oui dans ce processus de signature.

JACQUES LATOUR: C'est une très bonne question. Les registrer n'ayant pas un rôle important avec DNESSEC, il n'y a pas de valeur ajoutée au registrer DNESSEC. Donc c'est un problème qu'on a au Canada pour .ca, on a environ 180 domaines qui sont signés. La raison, je pense que seulement 1 registrer sur 180 supporte DNESSEC, ils ne sont pas intéressés, c'est un coût supplémentaire dans leurs opérations. Donc on est en train de chercher de nouvelle méthode pour signer les noms de domaines sans utiliser de registrer.

C'est mercredi à la session DNSSEC Workshop, si vous venez nous parlerons de ça à ce moment-là.

DAN YORK: Est-ce qu'il a répondu à votre question de façon correcte ? Oui si on a des gens qui voudraient parler allemand, je pourrai les aider.

(inaudible) Du Mali, juste une question rapide, est-ce que ICANN publie aujourd'hui une liste des registrer qui supportent DNESSEC pour les gTLD ?

JACQUES LATOUR: Pour les gTLD, c'est obligatoire de supporter DNESSEC. Est-ce que les registrer doivent soutenir le DNESSEC ?

INTERVENANT INCONNU: En fait ma question c'est est-ce qu'il y a une liste qui est publiée et qui est mise à jour par l'ICANN ?

JACQUES LATOUR: Non, non, non, il n'y a pas de liste qui est publiée.

INTERVENANT INCONNU: OK, je vais encore parler en français, jamais 2 sans 3, je vais peut-être poser une question un peu difficile, parce que le DNESSEC j'ai eu l'occasion de travailler dessus à l'université et c'est une technologie qui a été publiée depuis plus de 20 ans (inaudible), mais qu'est-ce qui peine fondamentalement a ce que le DNESSEC ne soit pas déployé partout, y a plusieurs acteurs dans la chaîne, est-ce que ça bloque dans un acteur principalement ?

JACQUES LATOUR: En ce moment, ça bloque au niveau des registrer surtout. Ceux qui signent les noms de domaines ce sont les opérateurs de DNS, c'est eux qui vont signer les noms de domaine. Mais ils sont trop loin des registres pour pouvoir créer (inaudible). Donc les

registrer (inaudible) c'est un gros élément qui bloque, la technologie pour signer comme avec (inaudible) il supporte DNESSEC, Red Hat, il supporte DNESSEC dans la (inaudible) par défaut. Donc ça servait bien, mais le gros problème c'est les registrer.

INTERVENANT INCONNU: J'ai oublié de me présenter (inaudible) du Bénin

DAN YORK: (inaudible) Mike, on a de la traduction.

THIERRY : Encore une question en français, je suis Thierry (inaudible) avocat au barreau de Paris. Je suppose que dans cette organisation de sécurisation du DNS, la société VeriSign fournit un certain nombre de produit et de service, et je voudrais rappeler l'importance du support de VeriSign pour développer la signature électronique dans le monde juridique. Aujourd'hui la signature électronique est utilisée par les juristes et les techniciens. Donc ma question est avez-vous des relations avec des juristes, est-ce que vos relations sont bonnes ? J'ajouterais aussi cela, c'est que l'Union européenne développe beaucoup de projets d'étude dans la sécurisation des échanges électroniques, qu'il y a un gros règlement européen 9102014 sur

les services de confiances qui sera en application dans toute l'Europe au mois de juillet et qui réglemente l'utilisation de la signature électronique dans tout le continent européen au niveau juridique et au niveau technique. Au niveau technique c'est l'institut européen des normes de télécommunication qui a fait le travail, ce sont des normes techniques qui sont acceptées par les juristes. Avez-vous des relations avec des juristes ?

DAN YORK : Je peux répondre en anglais. Vous avez soulevé un point excellent , je ne suis pas familier avec la législation qui se produit là-bas, je me souviens des gens qui se préoccupaient des politiques en discutaient, je vais donc retourner vers eux pour en apprendre un peu plus, il y a ici une opportunité pour voir comment le DNESSEC pourrait faire parti de cette discussion, merci pour cette suggestion. C'était très très bon, et nous allons noter cela pour obtenir des informations.

Nous avons parlé aux gens qui sont dans l'industrie du contenu, les gens dans le show-business par exemple, pour qu'ils puissent protéger leurs sites afin de s'assurer du contenu, je vous remercie.

JACQUES LATOUR: Je vais continuer en anglais. La discussion était autour des signatures légales, électroniques, pour pouvoir liées cela avec le DNESSEC. Dans l'avenir DANE, justement dont on parlait tout à l'heure, pourrait être un cadeau de travail pour permettre cela au niveau du DNS mondial. Je ne sais pas ce que nous devons faire pour cela, mais ça pourrait être une chose à faire potentiellement.

DAN YORK : Y a-t-il d'autres questions ? Une question de plus ?

OLIVIER : Bonsoir Olivier de (inaudible) du Congo. J'aimerais savoir pendant combien de temps on pourra détecter qu'un nom de domaine est déjà signé DNESSEC, parce qu'en atelier sur (inaudible), on a fait un petit atelier, et on s'est rendu compte que pour savoir qu'un nom de domaine est signé, il fallait installer un plug-in sur l'ordinateur pour savoir si effectivement il est signé DNESSEC ou pas. Alors j'aimerais ce qui bloque cela, pourquoi aujourd'hui certains outils n'ont pas la possibilité de détecter automatiquement comme on le fait avec le SSL ?

DAN YORK: Pourquoi n'y a-t-il pas moyen de voir dans un navigateur si le nom de domaine est signé. S'il faut utiliser un plug-in pourquoi

cela ne fonctionne pas autrement. Je vais vous poser une question, combien d'entre vous font attention au petit verrouillage vert qu'il y a sur votre navigateur ? Combien d'entre vous quand vous obtenez cette notice qui dit le certificat n'est pas correcte ou quelque chose comme ça, combien d'entre vous continue à cliquer pour continuer ? Oui voilà !

La trouvaille qui a été faite, c'est que la plupart des gens ignorent cela, on voit bien le petit verrouillage, mais s'il y a un problème avec le verrouillage on continue parce qu'on veut arriver au site en question. Donc (inaudible) un identifiant visuel que les noms de domaines utilisent pour prouver qu'il y a une signature ont été prouvé comme quoi cela ne fonctionnait pas, donc ce qui se passe dans l'espace DNESSEC, se passe en dessous de ce niveau-là. Si le nom de domaine a été signé, et s'il est bon, ça se voit, s'il est signé, mais il n'est pas bon, vous n'y arriverez pas. Vous allez obtenir ce que l'on appelle un échec, ce que l'on appelle nous un signal échec, vous ne pouvez pas atteindre le site, donc il n'y a pas d'interaction avec l'utilisateur, l'utilisateur ne voit pas ce signal, donc pour l'instant afin de voir si un site a un nom de domaine qui a été signé; il faut utiliser d'autres outils qui vous permettent de voir si le site a été signé.

Il y a des gens qui essaient de vous faciliter les choses, il y a un navigateur que l'équipe de Russ a développé qui fait cela, il y a des plug-ins comme vous l'avez dit qui fait cela, mais il y a une

espèce de division, il y a des gens qui auront utilisé ça, d'autres qui disent qu'on devrait s'assurer que telle ou telle chose est sécurisée. Je ne sais pas quand on va en arriver à ce point là. C'est comme une guerre de religion.

RUSS MUNDY: Comme l'a dit Dan, les recherches auront démontré que l'efficacité de mettre un indicateur visuel pour les utilisateurs était questionnable. Les gens veulent savoir où ils vont aller. Et aussi un autre contre argument, disons, c'est; est-ce que le DNESSEC est présent ou pas ? Beaucoup de gens veulent que cela vienne de système de défaut si vous voulez. Les chaques fois que vous avez besoin d'un indicateur, c'est quand le DNESSEC ne fonctionne pas, donc on voudrait en arriver à un point où on pourrait s'il y a un problème DNS quand il y a un échec du DNESSEC. Donc c'est pour ça qu'on continue à avoir ces ateliers d'apprentissage, pour que les gens puissent venir nous poser ces questions; pourquoi je ne vois pas l'information, il faut passer l'information, faite passer dans vos départements IT, vos fournisseurs.

DAN YORK: Nous n'avons plus le temps, il nous reste deux questions, je crois, mais si vous êtes intéressé pour avoir plus d'informations,

nous avons cet atelier mercredi et nous allons vous livrer plus d'informations à ce moment-là. Y a-t-il d'autres questions ?

NOMSA MWAYENGA: Je m'appelle Nomsa, je suis du Zimbabwe. Vous avez mentionné tout à l'heure le traffic de DNS africain. D'après vos observations, il n'y avait pas beaucoup de DNESSEC. Est-ce qu'il y a des moyens pour vous pour faire du renforcement de capacité ?Et comment allez-vous le faire ?

DAN YORK: Oui, une fois que la racine de DNS a été signée en 2010 beaucoup de TLD dans le monde ont commencé à signer. Mercredi matin, je vous montrerais une carte du monde, je vous montrerai le déploiement de DNESSEC, vous verrez beaucoup de cTLD african n'ont pas encore signés, il y a d'autre chose qui se passe en ce moment et qui change les choses, y a un monsieur qui a parlé de l'atelier tout à l'heure, atelier qui a été fait par l'ICANN, ISOC. Ces ateliers sont fait par l'ISOC, l'ICANN dans différents pays, ils essayent de travailler avec les opérateurs de registe, et d'autres acteurs dans les régions pour parler de la signature DNESSEC, est-ce qu'il y a des gens qui ont participé à ces ateliers ? Marc, oui ce monsieur y est allé aux ateliers travail, nous avons mis en place ces ateliers pour essayer de construire la dessous, si vous voulez. Si vous allez à dnssecafrica.org, c'est un site sur lequel

M.Alain Aina travaille et il y a des statistiques DNS qui montrent quels sont les pays qui ont signé et ceux qui n'ont pas signé. Il y a des liens aussi afin que vous puissiez apprendre plus de chose sur ce sujet.

Au verso de cette feuille, si vous ne l'avez pas eu, il nous en reste d'ailleurs, il y a une liste des ressources que vous pouvez utiliser, il y a des informations sur le déploiement du DNESSEC, sur les outils que nous avons utilisés et beaucoup d'autres informations que vous pouvez trouver sur internet. Voilà, vous pouvez commencer par ça si vous voulez, cela n'a pas le lien dnessec.africa je pense que nous n'avons pas encore eu l'occasion de le mettre là, mais c'est une bonne fihe à consulter.

Monsieur (inaudible) une autre question ?

INTERVENANT NON IDENTIFIE: Je suis du Maroc, est-ce qu'on peut dire que c'est l'une des raisons pour laquelle le DNESSEC est très lent dans son déploiement ? C'est parce qu'il y a d'autres outils qui nous facilitent la vie pour nous protéger conte les usurpations ? Il y a des usurpations à distance aussi et cela est rendu plus difficile n'est-ce pas ?

DAN YORK: La réponse à cela c'est que le déploiement se passe bien, nous en sommes à 20% du déploiement. Le problème c'est que le DNESSEC résout seulement une pièce du puzzle, du côté TLS, il y a d'autres technologies qui existent comme certains certificats, certains outils qui sont utilisés dans ce secteur, le DNESSEC résout son problème, sa pièce, son morceau du puzzle, d'une très bonne façon.

INTERVENANT NON IDENTIFIE: Est-ce que le DNESSEC va nous protéger contre l'usurpation sur internet, mais est-ce qu'on peut se protéger dans tous les environnements ? Si le déploiement du DNESSEC est si lent est-ce que c'est à cause de l'usurpation ?

DAN YORK: Je ne suis pas sûr, on peut parler plus longtemps. Il y a certainement d'autres méthodes d'usurpation de site, il y a d'autres mécanismes de protection, le DNESSEC résout ses problèmes de DNS, s'assure que l'adresse IP est correcte. Il y a d'autres sortes d'usurpation.

INTERVENANT NON IDENTIFIE: Vous devriez aller avec l'homme du milieu, il y a d'autres mécanismes pour résoudre ce problème.

DAN YORK: Je vous dirais qu'il y a certainement d'autres systèmes, DNESSEC c'est juste une partie de la défense. Pour nous sécuriser le DNS c'est ce qu'on fait. Une autre opinion, on a besoin que DNESSEC nous amène vers un internet de confiance, qui nous permet d'avoir toutes les opportunités que l'on veut et c'est l'outil qui nous permet de faire cela.

WARREN KUMARI: Beaucoup d'autre attaque genre l'homme au milieu. Toutes ces choses genre l'empoisonnement et tous ces autres systèmes d'usurpation, pour ce qui est de l'empoisonnement du DNS, si vous n'avez pas de DNESSEC, vous pouvez le faire dans beaucoup d'autres secteurs, à partir de n'importe où dans l'internet et vous pouvez avoir un impact sur beaucoup d'autres utilisateurs, donc l'ampleur de l'attaque peut être beaucoup plus importante. Vous avez besoin de beaucoup d'ensemble de protection, DNESSEC en fait partie.

DAN YORK: Il y a aussi d'autres mécanismes, qui sont des mécanismes dans lesquels on doit faire confiance à la première utilisation.

Donc avec cela, je voudrais résumer vite fait parce qu'on a passé le temps, je voulais vous donner cette fiche sur laquelle il y a les

liens pour avoir des ressources avec lesquelles vous pourrez apprendre plus, encore une fois il y a l'atelier le mercredi pour certains d'entre vous le début de cet atelier va être intéressant puisque nous allons parler des applications DNESSEC à travers l'Afrique, il y aura un panel avec Marc et d'autres personnes, Alain qui viendra parler du travail qu'il fait, donc cette partie de la réunion pourrait être intéressante pour certains d'entre vous.

L'ordre du jour est sur le site web et cet atelier, encore une fois, prendra place mercredi, nous espérons que nous serons à l'heure.

Je voudrais applaudir tous les gens qui sont là sur le panel et qui m'ont aidé à faire cette présentation. Nous sommes là encore quelques minutes si vous voulez venir nous parler. Merci.

[FIN DE LA TRANSCRIPTION]