BARCELONE – Atelier sur les DNSSEC (3 sur 3)
Mercredi 24 octobre 2018 – 13h30 à 15h00 CEST
ICANN63 | Barcelone, Espagne

RUSS MUNDY : Alors, nous sommes prêts à recommencer dans un petit instant pour notre atelier DNSSEC.

La première chose à faire, c'est déjà de remercier les sponsors du déjeûner. Je sais que moi, j'ai beaucoup apprécié. J'espère que c'est la même chose pour tout le monde. Donc c'est Afilias, .ca et SIDN. Nous les remercions.

JACQUES LATOUR : Bienvenue. Nous allons avoir un panel au cours de l'heure et demie qui vient à peu près, avec des présentations et discussions. Nous allons commencer par la présentation de Viktor d'abord sur le DANE.

WES HARDAKER : C'est Viktor Dukhovni qui a préparé certaines des diapositives. Moi, je suis Wes Hardaker de USC-ISI. Alors le titre n'est pas exact, c'est DANE et SMTP et l'utilisation ainsi que d'autres statistiques relatives au DNSSEC.

Nous allons passer en revue un certain nombre de choses. Je vais vous parler un petit peu de l'historique, comment fonctionne le SMTP. On parlera de la sécurité des courriels sans le DANE et avec le DANE,

pourquoi c'est mieux d'avoir le DANE. Et ensuite, on regardera des statistiques de déploiement de DANE que Viktor a collectées.

Alors je ne vois pas bien, cela ne va pas du tout. On pourrait peut-être présenter les diapositives différemment parce que là, on ne voit rien. S'il vous plaît, il faut réduire la taille, pas besoin de pouvoir déchiffrer le texte.

Lorsque vous envoyez un courriel, lorsque vous lisez un courriel, vous savez sans doute que vous avez quelque chose sécurisé, n'est-ce pas. Votre ordinateur envoie, un utilisateur envoie à son ISP en utilisant un mot de passe, cela passe par un SMTP TLS, cela arrive à votre FSI.

À droite, vous avez IMAP. Même chose avec TLS, connecté à votre FSI pour obtenir le courriel

Mais entre ces deux points, il y a un miracle qui se passe parce que entre les serveurs, ce n'est pas chiffré et n'est pas authentifié, c'est d'ailleurs fascinant de nos jours. Mais si vous envoyez ceci comme architecture dans un cours informatique, en général, vous auriez eu un F ou une très mauvaise note. N'est-ce pas ? Il faudrait être plus clair à l'étape deux.

Donc une solution en termes de sécurité des courriels, c'est de mettre en marche le TLS de manière opportune. Donc cela vous aide à éviter les attaques de l'homme du milieu mais cela demeure vulnérable pour tout ce qui est piratage BGP ou falsification de DNS, STARTTLS stripping, etc. Donc cela ne fonctionne pas parfaitement mais c'est quand même mieux que rien.

Alors, voilà là un diagramme du Gmail qui l'a fait. C'est sur le STARTTLS, sur leur croissance sortante à 90 % depuis le 11 octobre. Donc là, vous avez leur croissance STARTTLS entrante, donc cela arrive chiffré. Ce n'est pas authentique et c'est 91 %, vous voyez à droite sur le graphique.

Donc meilleurs objectifs de sécurité SMTP plutôt que de mettre en route le TLS. Il faut quand même être résistant à la mise à jour inférieure. Vous devez avoir un environnement mixte. Vous devez le signaler à vos paires et vous devez indiquer comment authentifier chaque paire.

Donc le SMTP, ce n'est pas comme le HTTPS. Vous allez sur un site avec le HTTPS et vous avez le choix si quelque chose se passe bien ou mal de continuer. L'utilisateur peut dire : « Oui, je vais continuer même s'il y a un échec. » ou alors : « Non, je vais éteindre parce que je n'aime pas leur CA. »

Cela ne fonctionne pas avec les hôtes de courriels parce que personne ne clique sur OK pour que la connexion se poursuivre. Donc on ne peut pas faire confiance à tout. Soit on fait confiance à tous les certificats pour interagir avec la personne, soit non. Donc voilà là où DANE est intéressant.

Dans les SMTP, la présence des enregistrements TLSA DANE indique plusieurs choses. Premièrement, il y a une compatibilité STARTTLS donc en principe, il devrait y avoir cette fonctionnalité. Si vous ne l'avez pas, cela veut dire que quelqu'un essaie de vous faire quelque chose qui n'est non chiffré alors qu'il faudrait que ce soit chiffré.

Également, les points de contact. Je ne vais pas rentrer dans le détail pour vous expliquer comment le DANE et le DNSSEC fonctionnent mais c'est un petit peu comme le DNSSEC. Tout le monde reçoit une indication que cela n'a pas été modifié.

Le DANE donne également au serveur SMTP quels sont les certificats ou les autorités de certificat qui auraient dû être utilisés pour signer le certificat que vous allez recevoir sur le SMTP.

Donc voilà pour aperçu général du DANE et comment on en est arrivé là, comment il protège. C'est en fait la solution pour vraiment protéger les courriels au premier contact. Il faut utiliser le DNSSEC pour y arriver.

Donc cela, c'est une pratique opérationnelle. Donc si vous déployez le DANE pour vous serveurs de courriels, voilà un petit peu quelques astuces pour démarrer. Moi, j'avais 35 diapositives. Il y en a 65 au total mais toute les informations de Viktor sont par la suite ; il y a beaucoup plus de détails. Mais là, c'est vraiment un résumé de haut niveau.

Premièrement, pour coexister avec DANE, il faut avoir des domaines signés DNSSEC, bien sûr. Sans DANE, ce qui se passe, c'est que si un site n'a pas DANE, s'il n'y a pas de déploiement de DANE comme beaucoup de personnes ne le font pas d'ailleurs, le support de déni d'existence du DNSSEC se produit : « Ils n'ont pas de DANE, donc pas besoin de s'imaginer que c'est sécurisé. »

Donc cela marche bien, DANE est le premier protocole qui demande le déni d'existence. Je ne sais pas si vous connaissez, c'est le NSEC, le

déni d'existence ; NSEC3, c'est ce qui rend ceci possible. Cela vous permet de savoir si oui ou non vous pouvez vous attendre à avoir une connexion STARTTLS sécurisée ou alors échec si vous ne l'avez pas.

Alors que se passe-t-il lorsqu'une recherche arrive à un échec ? Lorsqu'on est protégé par le DNSSEC, vous savez que vous passez sur les hôtes MX. Si on vous dit : « Cela ne marche pas ; je ne le fais pas. » alors à ce moment-là, vous savez qu'il faut vous arrêter, qu'il y a un problème.

Si tous les MX sont sautés, vous n'avez pas signé à temps par exemple, n'oubliez pas que le courriel, en fait c'est un protocole reporté, donc il n'y aura pas d'échec définitif.

Si vous adoptez DANE, la chose la plus compliquée, c'est en fait le DNSSEC parce que le DANE n'est pas compliqué en lui-même. Il y a la coordination des enregistrements de TLSA, cela peut sembler difficile mais il y a tout un tas d'outils qui rendent les choses faciles. Donc une fois que vous avez déployé le DNSSEC, déployer le DANE sur le serveur de courriel, c'est assez simple.

Pour le DANE sortant, si vous avez un agent de transfert de courriels avec DANE – donc Postfix, Exim, Cloudmark –, vous pouvez le mettre en route et vous devez avoir un résolveur validant le DNSSEC. Donc vous avez des documents MTA à lire là-dessus. Postfix par exemple, si vous avez un résolveur validant sur la même machine, pas de problème, cela partira tout seul. Ensuite, vous activez le DANE selon les documents, ce n'est pas compliqué, les configurations sont

simples. Vous pouvez le faire même si votre zone n'est pas signée, même si vous n'avez pas activé le DNSSEC ou le DANE.

Pour la partie entrante, il vous faut un serveur SMTP compatible avec le STARTTLS, vous devez avoir des enregistrements MX signés DNSSEC. Vous devez avoir des enregistrements TLSA signés DNSSEC pour chaque hôte MX.

Et si votre hôte MX est externalisé, donc moi, je sais que pour mon serveur, c'est le cas, il y en a qui externalisent, ovh.net par exemple. C'est justement une de ces connexions externalisée. Donc il faut qu'ils signent de leur côté. Donc les deux zones doivent être signées, la vôtre et celle de votre fournisseur. Et puis il faut vous assurer que vous avez une rotation des certificats et de clés gérée correctement.

Donc il y a un certain nombre d'outils DANE qui facilitent les choses. Vous pouvez aller chercher cette présentation bien sûr en ligne et vous pouvez trouver par exemple hashslinger, Paul Wouters est dans la salle d'ailleurs.

Il y a d'autres outils. Viktor Dukhovni a le danecheck. Et si vous n'avez pas encore installé ceci, il y a des notes à la fin des diapositives de Viktor qui vous expliquent comment l'installer. C'est un petit peu plus compliqué mais d'une manière général, ces outils sont assez simples. Donc voici mon serveur de courriels, dites moi quels sont les bonnes entrées DNS pour installer et signer et tout va bien.

Ensuite, je vais parler du sondage SMTP DANE de Viktor. Il a énormément travaillé pour collecter un certain nombre de

statistiques, courriels. Donc il s'occupe de la liste de déploiement du DNSSEC une fois par mois pour voir quels sont les résultats, non seulement sur le DANE mais sur le DNSSEC aussi. Donc tout ceci, c'est les données qu'il a collectées.

Une des choses qu'on me demande souvent ou qu'on lui demande souvent, c'est d'afficher ces données sur un site web pour pouvoir les consulter régulièrement et pas seulement une fois pas moi. Je n'ai pas envie d'aller les chercher dans mes anciens courriels.

Nous avons maintenant un site stats.dnssex-tools.org. Donc cela fonctionne, j'y étais justement ce matin. Il nous reste du travail encore à faire, ce n'est pas parfait, ce n'est pas complètement automatisé mais on s'approche de notre objectif. Notre objectif, c'est justement d'avoir des statistiques mises à jour au jour le jour pour voir comment son sondage analyse de DNSSEC et le DANE. C'est quelque chose qui a été fait en coordination par nous deux. Donc continuez de regarder ce qui se passe, nous allons améliorer les choses petit à petit. Mais vous pouvez déjà y aller, donc stats.dnssec-tools.org. C'est à la fois DANE et DNSSEC.

Voilà à quoi ressemble le site web. Vous voyez que le diagramme est très sympathique, déploiement de DANE. Vous avez cinq graphiques maintenant avec des chiffres également. Et le reste des données des diapositives y sont également affichées. Donc n'hésitez pas à aller voir ; dès demain, vous pouvez consulter les informations.

Dans son sondage DNSSEC DANE, il a surveillé les domaines délégués de suffixes publics, il a informé les opérateurs sur les problèmes de

rotation clé et certificat, il a également utilisé différentes sources de personnes extraordinaire, à la fois CZDS de l'ICANN, cette base de données, Verisign, l'accès ouvert de différents TLD, .se, .nu, .fr, .nl. Il voudrait avoir davantage d'information d'autres ccTLD. Donc je peux vous mettre en contact avec lui si vous le souhaitez ou alors le contacter directement. Et Farsight Security lui a donné également beaucoup de données.

Certaines des informations sur le graphique viennent justement de ces sources. Mais donc en fait, il couvre 200 millions de candidats de noms de domaine. Donc ce qu'il cherche à obtenir, c'est tout ce qui est DS, DNSKEY, MX, A, Quad A, TLSA. Et il collecte effectivement les chaînes de certificat d'hôtes MX, donc il essaie de voir quelles sont les correspondances.

Ensuite, les statistiques du sondage. Au 11 octobre, lorsqu'on en a parlé, on a mis les chiffres à jour donc c'est relativement actualisé. Il y a 8,95 millions de domaines avec un MX validé DNSSEC, donc c'est fantastique. Quand les gens me disent : « Le DNSSEC n'est pas déployé. » et bien, c'est vrai qu'il n'est pas partout mais c'est quand même un chiffre intéressant, un chiffre élevé.

Il y a 323 000 domaines avec le DANE SMTP. Donc on parlera de l'écart entre ces deux chiffres tout à l'heure. Il y a des millions d'utilisateurs, comcast.net, web.de, gmx.de. ; Comcast est un des plus grands fournisseurs qui a mis en marche le soutien DANE. C'était vous, n'est-ce pas ? [inintelligible] D'accord, donc les experts font partie de Comcast.

Il y a 5 538 hôtes MX DANE dans 3 641 zones. On en reparlera un petit peu plus tout à l'heure. Et il y a 500 domaines avec des problèmes de recherche d'enregistrement TLSA.

Donc lorsque vous avez une technologie qui est en cours de croissance, il faut évidemment voir où sont les problèmes. Cela, c'est vrai pour n'importe quelle technologie, que ce soit la sécurité ou non. Mais la sécurité est encore plus complexe donc il faut bien voir où sont les échecs.

Et ensuite, il y a 258 domaines avec de mauvais enregistrements TLSA ou aucun STARTTLS. Donc si vous avez un enregistrement TLSA pour votre serveur de noms, lors des connexions, il va falloir vérifier que vous êtes compatible avec le TLS. Et si ce n'est pas le cas, vous n'avez pas recevoir le courriel.

En ce qui concerne les premiers TLD, donc ce sont des domaines DANE en milliers. Félicitations aux Pays-Bas avec 3 millions, 935 pour le .com, 820 pour .se, etc. mais les Pays-Bas sont en tête.

En termes de fiabilité, les problèmes, c'est au niveau des domaines parkés. Ce n'est pas simplement des problèmes de DANE ou de DNSSEC mais c'est en fait qu'il y a un problème général dans la zone.

Déni d'existence, ce type de problème est uniquement sur 500 domaines. Et on verra une liste tout à l'heure avec un graphique de TLD avec une rupture basse. Toutes les statistiques sont sur notre site web mais les TLD pour lesquels DANE ne fonctionne pas est assez bas. Alors je suis désolé, il y en a un que je ne peux pas lire, mais il y a le .br,

0,04 %, ce qui est absolument extraordinaire parce qu'ils ont également un total très élevé. Donc même ils ont beaucoup de domaines... Est-ce qu'il y a des gens du .br qui sont ? J'aimerais bien vous parler parce que votre succès est extraordinaire. Viktor voudrait savoir comment vous avez fait. On a peut-être le temps pour vous poser la question. Est-ce que vous avez un système de surveillance, c'est cela ?

FREDERICO NEVES : Oui. Nous surveillons chaque délégation au jour le jour et nous signalons tous les mois. C'est comme cela qu'on s'assure que le chiffre reste bas.

WES HARDAKER : Donc en fait, vous parlez à vos clients enregistrés ? C'est cela ? C'est fantastique, extraordinaire. Très bon travail.

Le .hk : 0,06 % mais ils ont beaucoup moins de domaines enregistrés.

Donc il y a des TLD avec de gros problèmes, le .bank est un des plus élevées. Alors je ne sais pas s'il y a des gens de .bank, ne dites rien publiquement mais venez quand même me parler parce qu'on aimerait quand même savoir.

Ensuite, le .nrw, le .ru, donc problème assez élevé.

Toute la liste est sur le site web et même chose, elle sera mise à jour tous les jours. Donc voilà, la mise à jour est régulière.

Le nombre de domaine qui utilise le SMTP et DANE a beaucoup augmenté.

Alors attendez, j'essaie de voir un petit peu. Donc de 2016 à 2019, à droite, 325 000 domaines qui utilisent le DANE et le SMTP.

Alors, vous savez, j'avais dit que la plupart des gens externalisent leur domaine. Donc si vous regardez le diagramme d'après, le nombre de zones d'hôtes MX avec DANE, donc 3 600. Donc le nombre de serveur MX avec DANE est en fait bien moins important. C'est pour cela que le chiffre est aussi bas. Voilà le graphique dont je vous parlais.

La liste des domaines DANE bien connus ne fait que s'accroître. Viktor en a parlé à Porto Rico et à l'époque, il y avait la moitié de la liste que vous voyez maintenant. Il y en a certains qui sont plus importants, vous voyez la liste, comcast.net, dns-oarc. Tous ces des serveurs de messagerie sont très utilisés et très connus.

Il y a aussi des presque-domaines DANE. Ce que Viktor appelle des presque-domaines DANE, ce sont les cas où la zone est signée mais ce à quoi pointent les serveurs n'est pas signé. Et c'est le cas des gens qui externalisent leur serveur et qui se trouvent dans cette liste que je vous ai montrée. La zone originale est signée mais le serveur de messagerie ne l'est pas. Et c'est ce qu'on a à gauche, 4,5 millions d'enregistrements qui pointent vers des zones non signées.

La liste de Viktor doit être alimentée. Il y a de plus en plus de listes de délégations signées de ccTLD. Il aimerait avoir davantage d'informations pour alimenter cette liste et aider les gens justement

quand les choses ne se passent pas bien, qu'il puisse leur envoyer un courriel lorsque les choses ne se passent pas bien pour avoir de nouvelles données. Grâce à ces informations, il peut voir beaucoup plus d'informations.

Bien sûr, l'aide la plus importante, ce serait de résoudre les problèmes qui peuvent se poser au niveau de DANE, au niveau de la messagerie. Donc on vous prie de vérifier cela, vérifier les dénis d'existence. C'est quelque chose d'important au niveau du DANE parce que cela vous montre que vous êtes capable de faire ou non STARTTLS.

Et ensuite, si vous n'avez pas un domaine singé, vous pouvez utiliser DANE pour authentifier le serveur sans signer votre domaine si vous ne voulez pas le faire encore.

Et bien sûr, il faut autoriser DNSSEC et DANE, surtout avec les serveurs hôtes MX.

Comme je l'ai dit avant, il y a beaucoup d'autres diapositives après ; il y en a un tas. Vous voyez, il y en a un tas. Il y a beaucoup d'informations intéressantes pour vous, alors je vous invite à les lire.

Et on va garder les questions pour la fin du panel je crois ?

JACQUES LATOUR : Nous avons le temps pour des questions.

WES HARDAKER : Est-ce que quelqu'un a des questions alors ?

JOHN : Je n'ai pas une question, c'est plutôt un témoignage. J'ai vue le blog de Viktor qui m'a un peu grondé la dernière fois. Il y a des informations pour produire des enregistrements TLS et j'ai mis une heure à pouvoir mettre ces informations dans mes scripts. À chaque fois qu'on doit re-signer, on re-signe avec la même clé pour ne pas avoir à changer à chaque fois. Maintenant, j'ai 90 domaines signés avec des serveurs de messagerie.

Je sais que Viktor parfois, il a tendance à sous-estimer les difficultés, donc j'étais un peu surpris.

WES HARDAKER : Oui, c'est intéressant ce que vous dites. La deuxième diapositive de l'annexe est l'une des plus importantes. Cela s'appelle « Rouler les clés TLS » et il suggère deux manières de le faire. Mais vous avez raison. Quand le DNSSEC est apparu et DANE est apparu, ce n'était pas facile à utiliser. Maintenant, il y a des gens auxquels vous pouvez faire appel pour pouvoir générer les clés et les mettre en place. C'est beaucoup plus facile. Merci de cette question. Y a-t-il d'autres questions ?

JACQUES LATOUR : C'est plus une remarque. Ce que nous faisons à .ca, nous signons la liste de tous les domaines qui sont signés. Nous donnons cette liste à Viktor toutes les semaines.

WES HARDAKER : Et il apprécie beaucoup cela parce que ce n'est pas seulement un examen de statistiques. Il essaie de vraiment voir ce qui fonctionne et ce qui ne fonctionne pas.

Y a-t-il d'autres questions ?

JACQUES LATOUR : Très bien, merci.

[Applaudissements]

Maintenant, Peter Koch de DENIC qui va parler du déploiement de DANE en Allemagne.

PETER KOCH : Merci Jacques. J'ai quelques diapositives. Je pense qu'on peut voir les diapositives de Wes et je vais rentrer dans le détail par rapport aux diapositives que je vous ai déjà montrées. Alors, est-ce qu'on peut bien afficher la diapositive sur l'écran ? Très bien. Je pense que c'est bien.

Alors d'abord, il y a une petite erreur dans le titre. On ne devrait pas parler d'utilisations parce que je ne peux pas vous dire combien de connexions utilisent SMTP DANE. Wes en a parlé un petit peu, on ne sait pas vraiment combien de courriels passent pas des canaux sécurisés et combien ne le font pas. Donc il faudrait donc ne pas mettre ce mot « utilisations ».

Nous ne nous penchons pas sur les données comme le fait Viktor. On va parler de manière un peu plus générale.

Ce graphique, il n'est pas très clair. On ne peut pas faire la différence entre droite et gauche.

Pour ceux d'entre vous qui étaient là ce matin, je vous ai dit qu'on avait 16,2 millions de noms de domaine dont 100 000 sont signés. Ici, vous voyez les domaines qui utilisent DANE. Cela vous donne un petit peu une idée du tableau.

Mais si les noms de domaine de messagerie principaux sont signés, nous ne savons pas trop par rapport à cela. Wes a parlé de gmx.de et d'autres domaines qui sont signés. Mais ce serait intéressant de savoir combien de messages passent pas ces canaux sécurisés, le volume de messages qui sont transportés de manière sûre.

Ici, on voit un petit peu mieux. Sur les 100 000 noms de domaine qui sont signés, 86 000 ont au moins un enregistrement MX dans la zone apex ou racine. Pour ce qui est de la messagerie sécurisée avec DANE, Viktor et Wes appellent les autres domaines des domaines presque-DANE et on ne sait pas si à la racine il y a un enregistrement TLS ou non sur la partie droite du domaine de courriel. Cela fait 86 000 domaines qui sont dans cette situation.

Par curiosité, ici, quelles sont les cibles – je sais que Viktor aime beaucoup parler des paramètres TLSA. Alors je parlerai plutôt de distribution de type 1 et de type 3. On utilise les algorithmes Hash qui sont importants. Mais je vois, le plus intéressant, c'est au début où il y

a quelqu'un qui a pu obtenir l'enregistrement TLSA, EDNS0 jusqu'à ses extrêmes et puis les autres, c'est plutôt le paramètre 31. Si vous voulez, vous pouvez revenir aux autres diapositives pour voir les détails, mais c'est plutôt la situation générale.

Le nombre de cibles MX avec TLSA, ce n'est que 7 %. Ce n'est pas beaucoup. Nous avons examiné tous les domaines, on a commencé avec 86 000 domaines. Indépendamment de où pointent ces enregistrements MX, nous avons eu seulement 7 % de cibles MX avec des enregistrements TLSA. Il y a des améliorations à faire, bien entendu. On verra cela dans la prochaine diapositive. Ce qui veut dire que nous avons 1 300 cibles MX qui couvrent 28 000 domaines. On parle ici des domaines presque-DANE et les autres cibles vont ajouter d'autres 28 000 domaines.

Ça a l'air facile et quelqu'un l'a dit mais il y a des difficultés qui peuvent être sous-estimées. Vous vous rappellerez qu'on avait dit qu'une grande partie du déploiement du DNSSEC du côté signature est fait par les bureaux d'enregistrement pour leurs clients et qui pointent sur leur infrastructure de messagerie pour le système de messagerie. Dans ces cas, ils opèrent et ils signent les domaines de leurs clients et ils les pointent vers leur propre système de messagerie. Mais là où réside la messagerie n'est pas signé.

Donc en fonction de la taille du bureau d'enregistrement et de la complexité du système de messagerie, cela peut être difficile. Viktor a passé deux ou trois appels ou a envoyé deux ou trois courriels. Nous essayons de motiver les bureaux d'enregistrement ou leur suggérer

que cela pourrait être intéressant d'inclure tout cela. Mais bien sûr, il y a aussi d'autres facteurs non techniques qui peuvent empêcher le déploiement de ce type de solution.

Tout ne dépend pas de la partie technique. Parfois, il y a des facteurs politiques, surtout pour les grandes compagnies au niveau de leurs responsabilités, qui rendent les choses un peu plus difficiles.

Ensuite après, je ne veux pas répéter ce qui a déjà été dit. Nous voulons, donc, faire augmenter le nombre de ces domaines. Nous savons que il faut encore étudier le nombre de messages d'utilisateurs pour essayer d'avoir l'enregistrement MX dans le système. C'est assez facile, le maintien des processus pour le monitorage des roulements de clé, etc. John l'a bien dit, signer, resigner la clé, on peut ou pas vouloir rouler la clé. Quand tout cela est en place, cela requiert un effort supplémentaire. Mais des erreurs, bien sûr... Cela peut provoquer des dommages en ce sens qu'il y a des messages courriels qui sont perdus.

Il faut comprendre également que le déploiement de cela, si vous faites les choses bien et que vous surveillez le déploiement, c'est relativement facile. Mais tout ce qui est résolution de problèmes, cela s'avère à être beaucoup plus difficile. Pour ce qui est des problèmes qui impliquent le DNSSEC, cela est un peu plus difficile.

Il y a beaucoup de logiciels différents sur le marché et les gens ont réussi à faire pour la signature d'enregistrements MX avec différentes combinaisons de cache négatif ou des enregistrements TLSA qui ne suivent pas le chemin courant, etc. Ces cas-là sont bien plus difficiles à

résoudre lorsqu'il y a des problèmes. Et nous en avons parlé à plusieurs reprises dans ces panels.

Quand on parle de sujets qui requièrent l'intervention d'un expert, à ce moment-là, il y en a beaucoup qui font appel à Viktor.

C'est tout ce que je voulais ajouter par rapport à cette question mais vous pouvez avoir plus de détails techniques si vous avez le temps et si vous voulez poser des questions.

JACQUES LATOUR : Nous avons encore beaucoup de temps. Est-ce qu'il y a des questions pour Peter ? Russ, allez-y.

RUSS MUNDY : Peter, j'ai vu des informations dans un périodique il y a quelques mois sur une législation qui aurait été adoptée en Allemagne en ce qui concerne le chiffrement des courriels. Est-ce que j'ai mal lu ou est-ce qu'il y a quelque chose qui se passe dans l'espace politique, juridique qui justement pousserait cette utilisation à augmenter ?

PETER KOCH : Vous n'avez pas mal lu. Ce qui se passe, c'est que ce n'est pas une loi mais c'est que l'institut fédéral pour la sécurité de l'information a émis des directives pour le fonctionnement sécurisé des serveurs de courriels. Et il ciblait les FSI, les opérateurs de courriels, etc.

Alors cela n'est pas contraignant dans l'immédiat mais il y a une recommandation en ce sens. Et donc certes, cela a du poids et nous le savons dans ces cercles, BSI, c'est donc cet institut de sécurité, c'est comme cela qu'il s'appelle, le BSI, ils sont pour le DNSSEC et pour le DANE, ils sont vraiment pour. Et donc ils ont inclus ces éléments de protocole dans leur recommandations.

Encore une fois, ce n'est pas quelque chose qui est obligatoire dans l'immédiat mais il y a beaucoup de lois dans les technologies de l'information. Vous connaissez peut-être la directive européenne qui a été traduite en loi nationale. Il y a différentes clauses qui mentionnent – et je ne sais pas si j'ai le bon terme du point de vue juridique – mais bon, c'est un petit peu l'idéal. Donc cette remarque, bien évidemment, je ne suis pas un avocat et donc je ne peux pas vous donner les détails, ce serait dangereux. Mais merci, effectivement.

Du côté des politiques, Russ, vous avez raisons, c'est important. C'est cohérent avec ce qui s'est passé par le passé, c'est cohérent avec ce qui s'est passé aux Pays-Bas, etc.

RUSS MUNDY : Est-ce que vous avez pu détecter des choses qui point de vue technique, en fait l'impact de cette politique du point de vue technique ?

PETER KOCH : Non, par réellement parce que la raison, c'est que ce que nous mesurons ici, ce que je vous ai montré là juste à l'instant, c'est que

nous mesurons le nombre de domaines signés et de cibles MX. Et donc cela compte tous les grands FSI, tout le monde, même le mec dans son garage.

Donc tout ce qu'on souhaiterait avoir, c'est une idée du nombre de courriels qui se déplacent sur des canaux non chiffrés et sur des canaux TLS sécurisés DANE. Donc on n'a pas ces informations.

Ce que l'on peut faire, c'est que si les grands FSI l'annonçait – il y a d'ailleurs eu une initiative il y a quelques années de cela où des fournisseurs de mails allemands se sont rassemblés, je ne sais plus ce que c'était, ça s'appellerait *E-mail meet in Germany*, et donc ils avaient un canal chiffré entre eux, donc c'était un petit peu un cercle interne qui permettait d'augmenter les choses.

Et en plus, ils avaient chiffré leurs séances IMAP entre eux et entre leurs clients. Et encore une fois, on ne sait pas quel nombre de courriels se baladent mais c'est également intentionnel parce que les médias des technologies de l'information et les utilisateurs intéressés en parlent.

JACQUES LATOUR : Merci Peter. Des questions ? Oui.

JAAP AKKERHUIS : Je crois que j'ai déjà mentionné. Aux Pays-Bas, le gouvernement a des listes d'explications qui parlent de l'approvisionnement en service et du minimum. En fait, le DANE fait partie de cette liste de conformité.

Donc si vous voulez un contrat avec le gouvernement, si vous souhaitez répondre à des offres gouvernementales, et bien vous devez avoir le DANE. Donc en ce qui concerne les appels d'offre, apparemment, c'est important. Donc ce n'est pas simplement cocher la case et appeler son avocat ; c'est quelque chose de très important.

WES HARDAKER : Oui, Peter, je crois qu'il y a quelque chose que l'on n'a pas mentionné aujourd'hui. DANE, c'est un mécanisme générique pour la sécurisation des connexions, mais on parle du SMTP parce que c'est là que tout se passe. Est-ce que vous avez fait des mesures des serveurs de web ? Les navigateurs ne l'utilisent pas, donc est-ce qu'il y a d'autres protocole TLS que vous avez pris en compte ?

PETER KOCH : Non. Nous ne l'avons pas fait pour la raison évidente que les navigateurs ne feront pas le suivi de toute façon. Alors, il y a des gens qui le font parce qu'ils sont curieux, parce qu'ils aiment bien le DANE et peut-être bien même qu'il y a eu des surprises. Peut-être que les navigateurs ne restent pas fidèles aux informations du DNS, je ne le sais pas. Mais non, nous n'avons pas fait d'étude détaillée là-dessus.

WARREN KUMARI : J'aimerais mentionner qu'il y a à l'IETF une nouvelle proposition assez longue qui prend toutes les informations DNSSEC et qui y inclut tous les certificats, donc toutes les informations sont dans un certificat. Cela permet à un serveur web de le fournir à un navigateur. Donc les

navigateurs ne sont pas obligés de faire tout le travail DANE en plus, toutes les recherches DNS. Donc effectivement, cela peut être utilisé dans le cadre d'un certificat. Peut-être que les navigateurs pourront le faire.

WES HARDAKER : Vous savez s'il y a un engagement de la part des navigateurs ? Est-ce qu'ils sont prêts à le faire ?

WARREN KUMARI : Je ne sais pas. Je ne ferais pas de commentaires là-dessus. C'est possible.

JACQUES LATOUR : Et comment cela s'appelle ?

WARREN KUMARI : Une des raisons pour lesquelles les différents navigateurs n'ont pas utilisé le DANE jusqu'à maintenant, c'est qu'il faut faire plus de recherches DNS. Alors il y a des échecs parce que les recherches DNS parfois aboutissent à un échec. Et donc l'idée de cette proposition, c'est que toutes les informations sont dans un certificat dans une extension. Donc lorsque vous avez le certificat, vous avez toutes les informations DANE déjà. Et donc l'application n'est pas obligée de faire les recherches DNS elle-même. Et d'ailleurs à côté de moi, j'ai un expert qui est impliqué dans ce travail.

PAUL WOUTERS : Oui. Vous avez pratiquement raison. Avant, on mettait toutes les informations dans un certificat mais finalement, cela n'a pas été poursuivi. Donc maintenant, nous avons une extension TLS. Donc ce n'est pas un certificat. Mais c'est important quand même parce que c'est complètement séparé du web PKI.

Il y a certains navigateurs qui souhaitent l'utiliser mais il y a beaucoup de discussions au groupe de travail TLS, est-ce qu'on poursuit le travail. Ce sera peut-être neuf mois avec une nouvelle proposition. Si cela vous intéresse, il y a 1 500 courriels dans notre groupe de travail. Allez les lire, c'est très compliqué. Les gens sont intéressés, il y a un travail qui est en cours mais en fait, on est un petit peu en attente pour l'instant.

JACQUES LATOUR : Peter ?

PETER KOCH : J'aimerais maintenant poser des questions au panel. C'est lié au DANE, ma question. Si vous prenez la sécurité du transport des courriels comme sujet, je sais qu'il y a un travail à l'IETF sur la sécurité du transport pour le SMTP. Et si je me souviens bien, il y a un autre projet supplémentaire qui revient à signaler le transport dans le message ou au destinataire. Donc l'utilisateur, de temps à autre, se rendra compte que son courriel a été transporté de manière sécurisée ou chiffrée. J'aimerais bien avoir des informations si vous en avez

parce que les utilisateurs pourraient mieux comprendre à quoi cela correspond. La question, c'est de savoir s'ils font partie de cela. Est-ce qu'il faut qu'ils communiquent avec leur FSI ?

WES HARDAKER : Je vais en parler un petit peu de cette question, donc confiance à la première utilisation. Il y a une approche pinning. Lors de la première utilisation, l'utilisation n'est pas énorme mais si quelqu'un pouvait insérer un enregistrement MX, votre courriel pourra être pointé n'importe où. Donc si on pouvait avoir par exemple un empoisonnement du cache, si vous n'avez pas de DNSSEC en marche, on pourrait changer l'enregistrement MX. Et de toute façon, il pourrait vous livrer quelque chose, donc vous aurez une copie mais vous ne saurez pas que cela a été vu par quelqu'un aux Pays-Bas, donc c'est la pire des choses qui puisse se passer.

Donc lorsqu'on y a travaillé, c'est une attaque de l'homme du milieu, donc il faut commencer par le DNS. Donc lorsque vous avez l'enregistrement dans le DNS, tous les hommes du milieu, toutes les attaques seront évitées. Donc c'est en fait la meilleure solution technologique.

JACQUES LATOUR : Une observation. Donc c'est un petit peu la poule et l'œuf. Nous, on n'utilise pas le pinning de certificat avec le DANE parce qu'il n'y a pas d'enregistrements DANE qui puissent permettre de tester.

Si on ajouter davantage d'enregistrements, à ce moment-là, ce sera peut-être envisageable. Si nous signons plus de domaines, donc est-ce que le TLSA sera disponible ? Est-ce que le navigateur le mettra en route ?

WES HARDAKER : Vous avez dit deux choses, là. Si j'ai bien compris, si on publie les enregistrement TLSA pour les navigateurs web, peut-être effectivement que ce sera indiqué. Il y a quelqu'un, vous savez, qui observe et qui le mettra en route. Je ne sais pas si c'est la vérité. Il y a un navigateur qui utilise le DANE, n'est-ce pas ?

WARREN KUMARI : Si suffisamment de personnes publient les enregistrements DANE, il est possible que cette extension fonctionne. Il y a sans doute des navigateurs qui sont prêts à le faire. Mais à mon avis, les navigateurs ne feront pas tout ce qui est DNSSEC DANE. Il y a trop de latence et un certain nombre d'utilisateurs seront affectés. Donc les enregistrements TLSA, les enregistrements DANE, les certificats, les extensions, cela pourra peut-être fonctionner mais pour ce qui est des recherches DNSSEC, à mon avis, non.

WES HARDAKER : À un moment, on a parlé de leur montrer la page, de la charger immédiatement et quand il y a échec du DANE, on élimine la page.

WARREN KUMARI : Oui, c'était mon idée. Mais pour eux, c'est une mauvaise idée, c'est vrai parce que sinon, vous allez envoyer tous vos cookies aux mauvais sites. Et alors là, peu importe parce qu'ils peuvent quand même y arriver. En fait, c'était une erreur de ma part.

JACQUES LATOUR : Moi, ça me plaît cette idée, mais bon. Y a-t-il d'autres questions ? On a terminé ?

Présentation suivante de Wes à nouveau, donc racine locale.

WES HARDAKER : Une fois qu'on aura les diapositives, on commencera. Alors je crois que ma première demande serait qu'il faudrait qu'il y ait plus de personnes qui préparent des présentations sur l'atelier DNSSEC. Comme cela, vous n'aurez pas à m'écouter plusieurs fois. En tout cas, merci d'être avec nous.

Donc il y a à peu près un an, j'avais parlé d'un projet qui s'appelait la racine locale. Et l'idée de la racine locale, je vais vous l'expliquer mais là, c'est une mise à jour sur les nouveautés, sur ce qui s'est passé, de nouveaux éléments qui seront utiles. Et non, je n'aurai pas besoin de 20 minutes.

Voilà ici, vous voyez un peu une capture d'écran du site web. Nous allons entrer dans le détail dans une minute, si vous voulez y jeter un coup d'œil maintenant, localroot.isi.edu.

Pourquoi on a fait cela ? On devait faire un pré-cache d'enregistrement DNS. Au début, c'était seulement les données de la zone racine. Et je voulais faire un peu plus, j'en reparlerai.

Je voulais le faire très facile à déployer. Cela devrait être vraiment banal pour le déploiement, seulement copier-coller et pouvoir utiliser le RFC7706.Même si on ne voit pas très bien sur l'écran, c'est 7706 ; c'est un problème d'affichage.

Alors pourquoi utiliser des racines locales ? Je dois dire que cela fait un an que je l'ai fait. Ce que fait la racine locale, c'est qu'elle vous permet de copier la zone racine entière en pré-cache dans le résolveur. C'est assez facile à faire aujourd'hui mais il faut des notifications qui vous permettent de vous assurer que la connexion entre vous et le serveur que vous pointez est sécurisée.

En faisant cela, il y a un certain nombre de bénéfices. Notamment, vous accélérez le travail des serveurs locaux. Vous savez déjà la réponse donc vous ne posez pas de questions. Et c'est valable pour tous les enregistrements de zone, que ce soit DNS, DANE, etc.

Et cela prévient les pannes ou les échecs. Si vous avez une copie de la zone racine et que votre serveur racine est en panne, alors vous avez une copie. Une panne de zone racine n'est pas très fréquente mais il peut y avoir des pannes d'autres racines. Et cela reste utile.

Et ensuite, il y a la protection de la vie privée. Il y a eu une présentation. Je ne me souviens si j'ai fait cette présentation à l'ICANN où je montre que même si vous faites une minimisation des requêtes

et vous utilisez TLS, en posant des questions, vous êtes en train de libérer des données. Si vous posez une question par rapport à .ru, je sais que vous parlez de la Russie. Si vous parlez à .bank, je sais que vous travaillez dans le secteur bancaire, etc. Dons la meilleure façon de protéger la vie privée, c'est de ne pas poser des questions. Si vous avez toutes les réponses dans votre pré-cache, cela protège votre vie privée.

Le RFC7706, je vais faire un petit résumé. L'objectif principal de ce RFC est de donner des réponses plus négatives en cache, plus accélérées pour qu'il y ait moins de réponses sur le réseau.

Si vous vous souvenez de ce que je vous ai dit avant, dans notre ligne orange où il y avait des réponses un peu bidon, ce .com, si vous lancez une requête sur .com, vous allez obtenir ce type de réponse. Alors la plupart des requêtes vers la zone racine n'existent pas, je vous l'ai dit avant. Il y a des réponses négatives qui viennent tout le temps. Si vous posez la même question quelques secondes plus tard, vous aurez déjà la réponse dans le cache.

Si vous êtes dans une partie lointaine du monde, les choses s'accélèrent. Le trafic DNS est observable pour les tierces parties qui se trouvent sur le chemin. Donc qu'il y a possibilité qu'il y ait un filtrage d'informations par rapport aux noms de domaine sensibles. Ce que veut dire ce RFC, c'est qu'aucune question ne doit traverser le réseau.

Donc voilà quelles sont les nouvelles. J'ai changé le nom des clés TSIG et malheureusement, ces clés TSIG doivent être uniques et elles ne

peuvent pas changer. Je viens de les changer. Donc si vous utilisez la racine locale, il faut changer, il faut obtenir une nouvelle copie de cette clé. C'est la dernière fois que je le fais, je vous le garantie, je ne vais plus le refaire.

Maintenant, il est possible d'éliminer les serveurs non utilisés et les TSIG. Il n'y a pas de préférence de notifications par rapport à un nouveau compte courriel si je veux recevoir certaines informations. Je n'ai pas envoyé encore quoi que ce soit mais je vais le faire bientôt.

Pourquoi je présente cela ici ? C'est parce qu'avant l'existence du DNSSEC, ce projet n'aurait pu exister. Donc cela vous permet vraiment de pouvoir faire confiance à certaines sources.

D'autres zones peuvent être utilisées, .arpa et root-servers.net.

Il y a eu des améliorations au niveau de l'affichage du serveur. On peut voir le temps du dernier transfert. C'est une nouvelle fonctionnalité qui est maintenant active. On peut configurer. Il y a une touche de configuration à droite et il y a un *timestamp* que vous voyez et vous savez vers où pointent les copies. Il y a une meilleure génération de configuration, surtout au niveau de l'écran. Il y a donc beaucoup d'informations qui peuvent être saisies maintenant. Si vous voulez configurer partiellement ceci, vous devez saisir de nouvelles informations, cela peut contenir automatiquement votre adresse courriel. Si vous en avez d'autres, vous pouvez les inclure également. Il y a la possibilité de configurer de cette manière pour habiliter ces services. Et bien sûr, il y a un annuaire de stockage des fichiers de zone. Avant, cela n'existait pas, c'est une nouvelle fonctionnalité.

Ici, je vous montre un petit peu des choses que je voudrais faire. Il y a beaucoup de choses intéressantes à faire pour améliorer l'infrastructure. Maintenant, il y a un seul serveur DNS qui transfert les zones pour le moment. J'aimerais pouvoir arriver à avoir des multiples serveurs.

On ne supporte pas IPv6 encore. J'espère que cela va venir. Et j'aimerais pouvoir envoyer des notifications courriel. Quand vous ne pouvez pas faire un AXFR, vous devez éteindre et revoir ce qui se passe, même chose s'il y a un problème avec TSIG quand il y a un problème avec la clé. J'aimerais pouvoir vous envoyer des courriels.

J'aimerais pouvoir supporter Unbound et d'autres configurations de résolveur et d'autres sources de données DNS.

C'est ici le chantier le plus important pour moi, celui qui requiert plus de travail, pouvoir obtenir une liste de sélection. Si vous utilisez un TLD par exemple par rapport auquel nous avons des données, que vous puissiez les obtenir, ces données. Et donc peut-être que votre machine n'a pas la mémoire pour le faire mais vous ayez cette possibilité de tirer ces informations. Ce serait génial de ne jamais devoir à demander des informations parce que vous les avez déjà.

Il y a beaucoup d'informations que l'on doit encore collecter et tout cela, j'espère pouvoir le faire bientôt. Bien sûr, j'aimerais pouvoir publier tous ces codes pour qu'ils puissent être réutilisés.

Est-ce qu'il y a des questions ? Et si vous voulez rentrer, vous pouvez rentrer et si vous voyez l'URL, vous copiez la zone racine. Il suffit de

faire copier-coller. Et si vous avez des questions, je suis là pour y répondre.

JACQUES LATOUR : Oui, première question ?

JAAP AKKERHUIS : Maintenant, je me souviens de la présentation que je devais faire et que je n'ai pas faite. Vous avez parlé de Unbound et de la protection TSIG. Il y a différentes façons de faire les choses. Tous les serveurs racines... ce qui résout le problème, c'est que si vous vous connectez au reste du monde par satellite par exemple et qu'il arrive quelque chose, une tornade par exemple, du coup vous ne pouvez pas agir au niveau local, au niveau de la racine parce que l'information de la racine a expiré. Mais vous pouvez obtenir l'information d'un cache local, cela peut vous aider, au moins pour les communications locales. On dépend moins du fait des communications plus globales. Et c'est positif pour ce type de système.

WES HARDAKER : Oui, c'est un point très important. Et c'est l'un des objectifs du RFC que j'ai mentionné. Nous avons fait des recherches par rapport à cela, par rapport aux communications satellite, par exemple quand cette communication est perdue.

Vous avez raison, on parle d'un projet qui a été sponsorisé par l'ICANN pour pouvoir faire en sorte que les serveurs puissent tirer des informations aussi de ces copies de zones.

Et j'aimerais pouvoir aussi envoyer des notifications comme je l'ai dit pour que vous puissiez savoir où aller chercher les informations et pour que les TLD puissent régulièrement aller chercher ces informations.

ABDALMONEM GALILA : Bonjour. Est-ce que vous mesurez comment cela fonctionne ? Si j'ai par exemple ma zone racine locale, j'aimerais signer avec DNSSEC, quelle est la chaîne de confiance à ce point-là ?

WES HARDAKER : Alors, vous tirez la zone racine IANA avec leur clé. Vous ne changez rien. Le DNSSEC travaille de la même façon. Vous ne tirez pas une zone racine et vous faites une copie locale. Vous avez déjà interrogé la racine et vous avez les réponses. Il n'y a pas de différence de sécurité. C'est le même ensemble de clés.

ABDALMONEM GALILA : Et c'est la même ancre de confiance ?

WES HARDAKER : Il n'y a pas de différence.

ABDALMONEM GALILA : Je sais que c'est bien cela pour le blockchain, c'est un servie pour blockchain.

WES HARDAKER : C'est quelque chose de très différent. On pourrait en parler mais cela n'a rien à voir avec blockchain.

WARREN KUMARI : Alors, il y a du travail en cours à l'IETF pour que toutes les informations de la zone racine soient signées. Une fois que cela sera fait, pensez-vous qu'il faudra encore le TSIG pour le transport ou que cela pourra se faire en AXFR ?

WES HARDAKER : Oui, TSIG a l'air mieux mais si j'étais au milieu, je vous donnerais quelque chose de plus vieux. Avec TSIG, vous savez que vous avez la zone la plus mise à jour parce que vous pouvez faire confiance à cette chaîne de confiance.

DUANE WESSELS : Je voulais savoir comment celui qui prend la zone racine de vous, comment sait-on que c'est la bonne zone racine, la bonne copie ?

WES HARDAKER : Oui, c'est une bonne question. C'est grâce à DNSSEC. Cela n'aurait été possible sans DNSSEC parce que vous ne devriez pas me faire confiance, vous ne devriez pas faire confiance à mon serveur

autrement. Je pense oui, c'est grâce au DNSSEC et à la KSK que cela fonctionne et que vous pouvez faire confiance à ma copie de zone racine.

WARREN KUMARI : Quelqu'un pourrait essayer d'en créer une autre mais ce serait facile à voir parce que vous sauriez ; c'est une question de code. Je ne voulais pas continuer à parler. Vous devriez aller vérifier chez quelqu'un d'autre. C'est toujours plus vieux qu'un jour.

WES HARDAKER : La réponse pour vous deux, c'est qu'une fois que c'est fait, oui, la zone racine est l'endroit où il faut regarder.

BRETT CARR : Brett de Nominet. J'apprécie votre présentation et j'aime bien la possibilité de tirer les informations de votre copie de zone racine.

WES HARDAKER : Oui. J'ai parlé à beaucoup de gens et il y a beaucoup de serveurs racines qui font du AXFR et qui ont collaboré. Oui. C'est vraiment un système où vous n'aurez jamais un transfert de zone racine de quelqu'un d'autre.

ORATEUR NON-IDENTIFIÉ : Je crois qu'il est important d'avoir une certaine expérience opérationnelle par rapport à ceci. Et puis l'évolutivité, ce serait

important. À ce stade, c'est important de voir que le DNS est plus lié au contenu. Ici, on ne parle pas de quelque chose de contrôlé de manière centrale.

Il y a deux questions. On suggère d'étendre ceci au-delà de la racine pour les TLD, par exemple. Et la question serait alors comment pourriez-vous surveiller la qualité et non pas le contenu mais l'intégrité des données pour les TLD et la qualité de la transmission s'il y a des SLA en place pour certains TLD. Est-ce qu'il y aurait un changement là au niveau des exigences et au niveau des services pour les paquets DNS pour approvisionner la zone ? Est-ce qu'il faudrait des changements au niveau de la structure ? Parce que l'université de la Californie du Sud ne sera pas le seul endroit pour faire cela. Il peut y avoir des travaux en cours ailleurs pour voir cette question. Pouvez-vous nous en dire davantage ?

WES HARDAKER : Oui, ce n'est pas exactement cette expérience. L'infrastructure était plus importante. Mais l'idée, c'est d'être dans cet espace et la zone racine, c'est ce dont on parle le plus. Donc comment pouvons-nous donner à tout le monde ces données selon d'autres mécanismes qu'ils ont déjà ?

Donc moi, l'idée, c'était d'aller encore plus loin. Ce n'est pas uniquement la zone racine. Avec tout le DNS, vous avez déjà ce dont on parle. Donc c'est avant le cache. Vous avez raison. Je vous donne les choses à l'avance, cela change les attentes en matière de service. Mais une des choses que j'aimerais faire qui n'est pas sur cette liste,

qui est un petit peu plus loin, c'est d'avoir un test démon qu votre résolveur utilise déjà.

On devrait déjà avoir des choses qui permettent de s'assurer que le résolveur fonctionne. Maintenant, ce qu'on a, c'est qu'il y a échec et ensuite, on va vérifier. La question de savoir si le cache est une zone esclave pour ainsi dire ou de savoir si on y pointe à chaque fois, en fait, c'est de savoir où c'est.

Alors il y a deux questions. Je ne sais pas qui était premier.

ORATEUR NON-IDENTIFIÉ : Pourquoi est-ce qu'on ne propose pas une racine locale pour tous les FSI ?

WES HARDAKER : J'essaie effectivement de le faire pour les FSI, j'essaie de fournir cette racine locale. Alors avant de donner cela à tout le monde, assurez-vous que cela marche bien, mais c'est ce que j'espère. C'est quelque chose qui est sans doute utilisé dans des endroits plus petits, enfin dans des groupes plus petits. Pourquoi ne pas avoir ceci pour toute une région ? Il n'y a aucune raison que cela ne fonctionne pas.

DANIEL : Ce que je ne comprends pas, c'est où est la source. Est-ce que vous faite un AXFR ?

WES HARDAKER : D'où viennent les données, c'est cela ? Comme il a été mentionné, il y a une liste de serveurs qu'ils vous ont donnée, y compris pas mal de serveurs racine. Mais il y a des AXFR partout donc le B, le L, etc., il y en a plusieurs. Donc vous pouvez obtenir ces informations directement mais il y a également un serveur de racine locale où vous pouvez faire un transfert de racine locale.

DANIEL : Alors si j'applique cela au .com, vous pourriez avoir une sous-zone du .com avec signature RR7.

WES HARDAKER : Moi, je ne pourrais pas avoir des sous-zones sur une partie du .com. Mais je peux faire par exemple example.com ou ietf.com. Mais on ne peut pas faire tout le .com.

DANIEL : Non, pas tout le .com mais ceux qui ont signé.

WES HARDAKER : Une autre idée que j'ai eue, c'est un outil qui fasse une analyse artificielle, pas comme le font les racines locales mais avec un pré-cache. Parce que par exemple vous adorez ietf.org, donc vous allez toutes les heures vous assurer que c'est dans votre cache. Cela, c'est possible. Et on pourrait demander à l'intelligence artificielle ou à l'automatiste de voir ce qui fonctionne le mieux.

DANIEL : Oui, mais cela encourage les gens à signer leur domaine parce qu'ils seront pré-cachés.

WARREN KUMARI : Alors Joey Abley, moi-même et d'autres personnes – peut-être vous, même – nous avons parlé d'avoir un service où les gens s'inscriraient, donc un échange DNS où les gens pourraient envoyer leur fichier de zone dans un lieu, un point de transfert et tout le monde pourrait les rendre esclaves avec une option cache flush. On pourrait demander qu'il y ait un cache flush sur des zones spécifiques.

WES HARDAKER : J'ai 90 % de cette infrastructure pour vous déjà. C'est tout terminé.

WARREN KUMARI : On en discutera alors.

JACQUES LATOUR : Est-ce qu'on prendre encore une question ? Allez-y.

ABDALMONEM GALILA : Je ne sais pas si j'ai tort mais à chaque fois que l'ICANN essaie de resigner la zone, les FSI devraient avoir une autre version pour le serveur de zone. C'est cela ? Donc toutes les données sont cachées, donc…

Deuxièmement, peut-être que je ne fais pas confiance à mon résolveur. Donc j'ai ma copie mais à chaque fois...

WES HARDAKER : Par rapport à votre premier point, vous avez une nouvelle copie des données tout de suite. Cela, c'est un désavantage. Ce n'est pas aussi important pour la zone racine parce que cela ne change pas beaucoup. Mais dans les autres zones, il y a des mises à jour plus fréquentes, donc c'est plus important.

Pour la zone racine, il y a moins de changements. Lorsque les nouveaux gTLD arriveront, vous allez en avoir un tout de suite et personne ne va aller le chercher et les nouveaux gTLD, il y aura un certain temps pour les mettre en marche, etc. Donc les signatures, vous les aurez tout de suite aussi, oui. Tout le fichier de zone, vous le recevrez, y compris les signatures. Donc vous aurez toujours la toute dernière copie en quelques secondes.

Et c'est une autre chose que j'avais sur d'autres diapositives, donc de permettre aux chercheurs de faire des recherches en terme de fréquence des mise à jour des zones parce qu'on n'est pas toujours obligé d'aller toujours chercher la zone racine pour savoir si les mise à jour ont été faites. Vous aurez des informations, il y aura propagation, il y a tout un tas de systèmes, mais c'est en quelques secondes de la mise à jour de la zone racine que vous serez informés. Donc ce n'est pas synchronisé plusieurs fois par jours ; la mise à jour en fait varie.

JACQUES LATOUR : Comment est-ce que cela marche sur la racine locale ?

WES HARDAKER : Le RSSAC réfléchit à certaines options. Donc dans le reste de l'ICANN, cette technologie est appelée une racine locale hyperlocale. Donc lorsque que vous avez une copie de la zone racine, aucune des données ne rentreront dans le DITL. Et donc si le monde entier avant des racines locales, la racine DITL, il n'y aurait rien. Il y a des gens qui pensent que c'est un problème, d'autres qui pensent que c'est un avantage.

JACQUES LATOUR : L'idée, c'est de ne pas perdre de vue ce qui se passe, Firefox peut-être ; je ne sais pas, peut-être qu'en fin de compte, on les aura.

WES HARDAKER : Je ne sais pas si c'était vous, mais on avait quelqu'un du .ca qui était intéressé et qui souhaitait utiliser la même chose. Donc voilà pourquoi je souhaitais publier le code, parce qu'ils voulaient que leur FSI ait le .ca pré-caché. Si le .ca a le DDoS, peu importe. C'était vous ? Ah, c'était vous. Bien, on peut continuer de travailler dans ce sens.

AHMAD ALSADEH : Je suis boursier. Il me semble que l'instance de la racine résoudrait le problème de la racine locale. Plutôt que d'avoir une racine locale, on pourrait avoir un serveur racine près de l'infrastructure plutôt que d'avoir une racine locale, donc. Je ne sais pas si vous êtes d'accord.

Sinon, ne pensez-vous pas que votre projet affectera le nombre d'instances de serveur racine ?

WES HARDAKER : Excellente question. Deux choses. Premièrement, oui, vous avez raison. Si vous aviez une instances des opérateurs des racine à côté de votre boîtier, vous n'en aurez pas besoin, effectivement. Mais on n'en arrivera jamais à un point où il y aura suffisamment de matériel qui pourra être envoyé à tous les FSI de la planète. Ce n'est absolument pas envisageable. Donc cela permet aux FSI d'utiliser un équipement qui existe sans rien acheter de neuf et d'installer une copie localement.

AHMAD ALSADEH : Et qui fait le routage ? Est-ce qu'il faut aller à l'extérieur ? Est-ce qu'il doit retourner vers ce serveur de racine locale ?

WES HARDAKER : Effectivement, bonne question. Si vous avez une instance près de vous, le logiciel de serveur de noms n'utilise pas toujours le même boîtier alors que si vous avez une racine locale, étant donné qu'elle est juste là, en général, les demandes ne sont pas faites à l'extérieur du boîtier. Si vous avez une instance, en général la requête est envoyée ici en général.

RUSS MUNDY : J'ai une question pour Wes. Lorsqu'on aura une meilleure définition du type de statistiques, du type de données qui sont nécessaires, qu'il faut collecter du serveur racine pour avancer, est-ce que vous allez incorporer certaines de ces informations des sous-ensembles ? Les informations sont disponibles au fur et à mesure que les instances 7706 se présentent ?

WES HARDAKER : Je ne savais pas qu'il y aurait autant de questions là-dessus. Effectivement, bonne question. Avec le DNS-OARC, pourquoi pas ne pas contribuer aux données. Et effectivement, le RSSAC002, c'est tout à fait possible. Alors je vais peut-être l'ajouter, je n'y avais pas pensé. Il faudrait que je trouve un financement pour quelque chose d'aussi important mais tout à fait, pourquoi pas.

WARREN KUMARI : Si vous aviez mes données de mon instances locale, est-ce que cela vous intéresserait ?

WES HARDAKER : Est-ce que vous y feriez confiance ?

WARREN KUMARI : Vous voulez du financement ?

JACQUES LATOUR : D'autres questions ? Très bien, merci.

Merci à tous.

[Applaudissements]

WES HARDAKER : N'oubliez pas : faites vos propres présentation, comme cela, je n'aurai plus à prendre la parole la prochaine fois.

RUSS MUNDY : Et bien, merci à notre panel DANE, merci à toutes les questions, la discussion est intéressante. C'est une des raisons pour lesquelles nous organisons ces séances, non seulement pour savoir un petit peu ce qui se passe dans la communauté puisqu'il y a des gens qui sont sur le terrain, qui font le travail et qui parlent de ce qu'ils font, mais l'idée, c'est aussi d'avoir du feedback sur ce travail et aussi sur de nouvelles idées, de nouvelles fonctionnalités qui sont suggérées par la communauté dans son ensemble.

Pour moi, la séance a été excellente. Je ne sais pas, peut-être qu'il faudra revenir en arrière sur le tableau de Viktor pour voir si l'utilisation du DANE a augmenté par rapport à la dernière fois où nous avons fait l'atelier. Est-ce que vous le savez, Wes ?

WES HARDAKER : Non, je ne sais pas mais il y a une personne qui a déployé la racine locale, elle fonctionne, elle est vérifiée. C'était vous ? Non, ce n'était pas vous. Il y a quelqu'un dans la salle qui l'a fait. Très bien.

RUSS MUNDY : Merci à tous les intervenants. On les applaudit.

[Applaudissements]

Alors, situation intéressante puisque la salle Adobe Connect fonctionne, me semble-t-il. Enfin, ce n'est pas sûr.

ORATEUR NON-IDENTIFIÉ : Par contre, pour les présentations, cela ne fonctionne plus.

RUSS MUNDY : Alors dernière partie de la discussion, les gens dans la salle pourront réfléchir à ce qu'ils ont entendu aujourd'hui, ce qui les intéressent particulièrement. Et l'idée, c'est de donner aux gens l'opportunité de penser à ce que vous souhaitez qu'on mentionne la prochaine fois. Nous avons ces ateliers à chaque fois et donc il est certain que nous en aurons un lors de l'ICANN64 et on souhaite que vous repartez d'ici non seulement en réfléchissant à ce que vous souhaitez entendre mais à ce que vous souhaitez nous présenter.

Donc merci Wes, vous l'avez mentionné tout à l'heure, nous avons besoin de davantage d'intervenants. Et nous allons envoyer un message au début de l'année. Donc il y aura un appel à participation, donc regardez bien vos courriels, on l'envoie par le biais de plusieurs listes de diffusion, donc dites-nous ce dont vous voulez parler lors de la prochaine réunion.

Par rapport à ce dont on a parlé aujourd'hui, tout le monde a un peu sa propre spécialité dans l'espace DNS, la structure est très large. Donc pensez un petit peu à votre impact, est-ce que vous avez un impact sur la zone si vous en détenez une. Et dans ce cas, signez vos zones, publiez-les comme zones signées, travaillez avec votre bureau d'enregistrement si vous travaillez avec un bureau.

Et nous en sommes à un certain succès avec le domaine DNSSEC dans la communauté des bureaux d'enregistrement parce que si votre bureau ne fait pas le DNSSEC, vous pouvez parfois les convaincre. Donc vous pouvez déplacer des noms d'une zone à l'autre. Et je dois dire que personnellement, je l'ai fait une ou deux fois parce que le bureau d'enregistrement n'utilisait pas le DNSSEC ; donc cela, c'est quelque chose qui est possible.

Envoyez vos statistiques, travaillez avec ceux qui font de la recherche. Nous souhaitons réellement avoir autant de personnes que possible impliquées. Nous avons un certain nombre d'entreprises, pas énorme mais un certain nombre d'entrepreneurs qui ont des signatures DNSSEC sur leur zone publiées et parsons.com justement, qui est un grand acteur, en fait partie et fonctionne comme zone entreprise signée.

Nous avons également les opérateurs avec qui nous fonctionnons, non seulement les bureaux d'enregistrement mais les serveurs de noms parce que souvent, c'est externalisé ; nous en avons parlé aujourd'hui.

Donc trouver des moyens pour que davantage de personnes signent. Si vous êtes FSI, un fournisseur de service, nous avons dans la salle des personnes qui sont FSI qui souhaitent en faire plus, donc très bon feedback, encouragez les gens à le faire. Ce groupe, cette communauté DNSSEC est une excellente communauté depuis les 15-20 années passées, surtout en termes de partage des informations. Les gens sont toujours prêts à communiquer les informations. Donc restez en lien les uns avec les autres. Si vous voyez besoin d'aide, n'hésitez pas à le demander, les gens vous aideront.

Ceci étant, nous n'avons pratiquement plus de temps.

MATT : En ce qui concerne les présentations, est-ce qu'elles seront chargées quelque part ?

RUSS MUNDY : Elles y sont déjà.

MATT : Ah, j'ai rechargé le site, je n'ai pas vu la présentation de Wes.

RUSS MUNDY : L'atelier DNSSEC, étant donné la structure des réunions de l'ICANN, est en trois parties. Vous avez la partie 1, la partie 2, la partie 3. Alors [Patrik] n'avait pas de diapositive donc il les enverra et vous les aurez par la suite.

Très bien. Y a-t-il d'autres commentaires ? Des questions ?

JACQUES LATOUR : Je voulais savoir s'il y avait des sujets qui vous plairaient pour la prochaine fois pendant qu'on y est ?

RUSS MUNDY : Oui. Est-ce qu'il y a des sujets spécifiques que vous souhaitez proposer pour que le comité des programmes y réfléchisse pour la prochaine fois ?

ORATEUR NON-IDENTIFIÉ : Le DNS qui utilise le blockchain.

RUSS MUNDY : Nous allons l'inclure dans la notre appel à participation. Très bien. Effectivement, pourquoi pas. Une autre ici ?

ORATEUR NON-IDENTIFIÉ : Un progrès du navigateur, la recherche, l'exécution.

WES HARDAKER : Le monde de la recherche sur le web et son interaction avec le DNSSEC et le DANE.

RUSS MUNDY : D'autres suggestions ?

JACQUES LATOUR : J'ai une question. Pourquoi n'y a-t-il pas des questionnaires DNSSEC cette année ?

RUSS MUNDY : La réalité, c'est qu'on avait tellement de choses à faire que cette fois-ci, nous n'avons pas inclus le test. Il y avait trop de choses à dire.

JACQUES LATOUR : Ou alors, si on trouve un volontaire qui veut bien organiser le prochain test.

WES HARDAKER : Moi, j'ai encore une question que j'ai gardée pour la prochaine fois, une question piège.

JACQUES LATOUR : On aura un test la prochaine fois.

RUSS MUNDY : Encore une fois, merci aux sponsors de notre déjeûner, Afilias, .ca et SIDN. Merci à tous les intervenants. Vous recevrez un appel à participation. Merci à tous.

[FIN DE LA TRANSCRIPTION]