KOBE – Atelier sur les DNSSEC (3 sur 3)
Mercredi 13 mars 2019 – 13h30 à 15h00 JST
ICANN64 | Kobe, Japon

JACQUES LATOUR: Bonjour, bon après-midi. Est-ce que nous sommes prêts pour commencer ? J'espère que vous avez tous fait un plaisir pour le déjeuner. Je remercie les sponsors. Il y a beaucoup de sponsors. Mais avant de commencer à les nommer : Afilias, JPRS, VeriSigne, Cloudfare, AuDA, NIC br, GoDaddy, Cira, Donuts, et d'autres.

C'était bien. Merci donc à tous.

NON IDENTIFIE: Le déjeuner n'est pas gratuit pour eux, mais pour nous. Donc oui, c'est très bien.

JACQUES LATOUR: A Marrakech, nous aurons des langoustes à manger. Maintenant nous allons aborder la question de l'avenir de la KSK. Nous allons parler de la fréquence du roulement de la clef. En fait, il s'agit d'un sous-thème. Et je cède la parole à Paul.

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

PAUL HOFFMAN: Bonjour, je travaille à l'organisation de l'ICANN, je travaille dans le bureau du directeur des technologies. Vous dû assurément nous voir avec mon chef ici, dans d'autres réunions liées à la question du roulement de la KSK.

Maintenant nous allons parler de ce qu'il va se passer dans l'avenir.

Ha… Que c'est bien ce petit outil que j'ai pour pointer !

Bien, donc, parlons un tout petit peu de la présentation. J'ai quelques diapos seulement, et ensuite je serai disponible pour les questions réponses.

Je ne suis pas là pour diffuser une doctrine, ou pour prêcher une doctrine mais pour parler avec vous.

Pour ceux qui ne le savent pas parmi vous, il y a eu des séances ce matin sur le DNSSEC, vous connaissez fort probablement la plupart des notions. La question du roulement de la KSK est en cours depuis 2015. Le 11 octobre 2018, on a la sensation qu'il y a un siècle, mais ce n'était pas comme cela, nous avons cessé de signer la clef, la clef précédente a cessé de signer l'ensemble des clefs. Et on a commencé à signer les autres clefs.

À ce moment-là, nous ne savions pas ce qui allait se passer, il y a eu beaucoup de signes de conflits. Je vais vous montrer après une

diapo à propos de cela. Mais on a trouvé beaucoup de choses étonnantes dans ce processus, avant octobre.

Et pourquoi est-ce que je dis tout ça ? Parce que cela a un effet sur notre façon de voir, sur ce que nous allons faire de la KSK dans l'avenir.

Si tout cela vous intéresse, toutes ces choses étonnantes qui se sont passées se trouvent dans un White Paper qui est dans l'URL que vous voyez sur l'écran.

Donc pourquoi sommes-nous là ? Voilà. Non seulement pour dire j'aimerais bien faire cela, mais aussi parce que, comme nous savons ce qu'il s'est passé et nous savons ce qui continue à se passer, nous voulons voir comment cela va porter un effet sur notre manière de voir le roulement de la KSK.

Nous voulons avoir davantage d'opinions. Et je vais vous montrer après comment cela va se faire.

Il y a eu plusieurs commentaires, pour ceux qui ont suivi le débat. Si quelques personnes vous donnent leur opinion, ne pensez pas que c'est la seule opinion, et ne pensez pas que toutes les opinions sont les mêmes. N'ayez pas cette sensation qu'il y a une unanimité ou un consensus ferme au sein de la communauté autour de ce sujet. J'aimerais que ce soit le cas plus tard, mais pour que cela puisse se produire, il faut en débattre.

Donc maintenant parlons de la manière dont les prochaines mesures vont être prises. Il y a un débat sur cette liste de diffusion. Si vous n'êtes pas sur la liste, vous pouvez y adhérer, vous pouvez consulter les archives. Jusqu'ici il n'y a pas eu trop de discussions, le volume était raisonnable. Et vous pourrez participer à la liste. La liste de diffusion est le mécanisme de préférence pour le débat. Nous allons continuer à débattre de ceci pendant cette quarantaine de minutes. J'espère bien qu'il y aura un débat, je ne veux persuader personne.

Ce qu'il y a de plus important par rapport à nos opinions c'est que le débat ou les déclarations qui sont faites, seront faites dans un espace contrôlé.

Il est très important que lorsque ce processus de débat est fini il n'y ait pas 30 ou 40 personnes qui disent : moi je veux ceci. Mais que nous ayons cette situation : écoutez j'écoute ce que vous dites, mais je ne pense pas que cela doit se passer de la sorte pour telle ou telle raison.

Nous voulons voir comment évolue la discussion. Il se peut que je sois un peu un rêveur, mais la liste de diffusion technique n'est peut-être qu'une liste, mais étant donné l'important du DNSSEC, des DNSSEC pour le DNS, ce serait superbe que la communauté se mette d'accord après un débat.

Ce serait très utile, ou ce serait bon pour vous de prendre la parole, même si vous n'avez pas l'obligation de le faire. Mais c'est tout à fait acceptable si vous voulez répéter aujourd'hui ce vous dites sur la liste de diffusion, ce ne sera pas considéré comme une répétition. Parce qu'il y a un petit groupe dans cette salle qui est très actif pour cette analyse de la KSK.

Ce que vous direz aujourd'hui, ce serait super de le mettre sur la liste de diffusion pour le reste des personnes puisse y répondre.

Une fois fait ceci, une fois fini le débat ici, dans d'autres forums dans les mois à venir, pendant la deuxième moitié de l'année, nous ferons une révision de ce thème de cette discussion, ce que nous dirons aujourd'hui, sur la liste de diffusion et dans d'autres réunions et on fera une proposition.

Nous ne savons pas encore comment cela va se faire. Nous ne savons pas si cela va se faire par l'intermédiaire d'une communauté formelle ou informelle ou d'une table de discussion, et par l'intermédiaire de l'IANA.

Pour que ce soit clair, je ne fais pas partie de l'IANA, je fais partie du bureau du directeur de la technologie.

Il y a toutes ces activités qui concernent la transition récente, mais c'est l'IANA qui, disons, clique sur sa souris, et c'est elle qui fait prendre toutes les décisions, et ce sera toujours l'IANA qui

continuera à le faire. Même si je modère et que je conduis la réunion, c'est l'IANA qui prendra bonne note de ce que vous aurez dit dans cette réunion, et c'est eux qui mettront en œuvre cela, et c'est eux qui définiront le plan de ce qui sera fait dans l'avenir.

Pour que ce soit bien clair, il n'y a pas de plan pour le moment pour l'avenir. On rédige la déclaration de la KSK qui dit que l'ICANN devrait faire le roulement de la clef tous les 5 ans. Ce délai a commencé le 11 octobre 2018. Ceux qui sont bons pour les maths, il faut que vous y réfléchissiez, on a commencé en 2010 et le roulement de la clef n'a pas eu lieu avant la fin de 2018. Donc la phrase : au bout de 5 ans, a été prise littéralement en ce sens qu'il ne fait pas faire le roulement de la clef avant 5 ans, mais il faut faire le roulement de la clef au moment où l'on a eu 5 ans et une minute.

L'IANA n'est pas conduite de la même manière que l'ICANN, avec une approche du bas vers le haut ; mais en tant que communauté nous voulons faire quelque chose de rapide, nous voulons que l'IANA nous écoute. Et ce texte, au bout de 5 ans, peut changer. Ce n'est pas quelque chose de figé.

Nous avons vu qu'il y a eu plusieurs modifications au cours de ces 8 années. Donc ce que vous aurez dit sera considéré et analysé aussi bien par l'IANA que par la communauté. Et il y aura un résultat à partir de cela.

Ce que je vous disais donc, c'est qu'à un moment donné de la deuxième moitié de l'année, les choses se feront une fois finie cette discussion. La liste de diffusion, encore une fois je le dis, ce sera le meilleur espace pour ce type de discussions.

Vous n'êtes pas obligé de présenter une déclaration bien préparée. Et enfin, quand vous aurez mémorisé vous pouvez prendre le temps et aller sur la liste. Si vous n'êtes pas anglophone, bon ce n'est pas mon cas je suis un américain natif, je ne parle que l'anglais, mais vous, vous pouvez prendre votre temps pour vous exprimer.

Donc j'ai ici quelques diapositives pour vous dire pourquoi nous voulons commencer une discussion sur ce qui s'est passé après octobre 2018.

Là vous avez un graphique du volume de requête de la DNSK. Ce n'est pas tout à fait exact, mais c'est une approximation assez bonne.

Notre attente est qu'avec le temps, le même nombre de résolveurs feront les requêtes. Dans des circonstances normales, on dirait : bon il y a deux jours que ces DNSSK, j'ai besoin d'une autre copie. Dans le monde idéal, ou dans le monde raisonnable, cette ligne verte qui est en bas, représente environ un millier, et cela devrait se poursuivre tout au long de la période. Nous pouvons voir que ce n'est pas le cas. La première barre rouge

représente le roulement. Comme vous le voyez, c'est à peu près en octobre, vous le voyez en bas à gauche.

Mais à un moment donné un groupe de résolveurs commence à envoyer des requêtes de la DNSKey à la racine, de manière plus fréquente qu'auparavant. Et comme la plupart d'entre eux n'avaient pas commencé à le faire, cela signifie qu'un petit nombre de résolveurs envoient des requêtes. Et c'est un résultat inattendu.

Il y a beaucoup de théories sur ce fait et ces raisons. Les premières théories disaient que cela allait se passer pendant deux jours seulement, et que cela s'arrêterait après, mais cela n'a pas été le cas.

Donc, DNSSEC à proprement parler, est un protocole assez régulier. Mais la manière dont il est mis en œuvre dans les résolveurs est assez étonnante.

Pour avancer rapidement aux deux autres barres rouges, à savoir le 11 janvier de cette année, il y a à peu près 2 mois, on a révoqué la vieille clef. Cela signifie que la vieille clef est publiée dans la racine, mais son accès a été annulé.

Et même après cet énorme saut, c'est un non-événement, cela ne… Regardez là, une fois qu'on a dépassé la deuxième barre rouge… Bon cette diapo est un peu ancienne… Même après la

deuxième barre rouge à droite, cette courbe continue de monter, et continue de monter. Elle a même augmenté un peu plus.

Donc si on réfléchit, on pense au roulement. Qu'est-ce que nous allons faire ? Nous allons faire X ou Y parce que nous savons qu'il y a quelque chose qui se passe. Pensez aux cas où il y a des défaillances, pensez si nous voulons allez plus vite ou plus lentement.

C'est un séisme ce que j'ai senti… Je demande ça aux Japonais.

YOSHIRO YONEYA: Ne vous mettez pas debout.

PAUL HOFFMAN: Pour que ce soit bien clair… En Californie, nous faisons les choses autrement. En Californie, on se met sous le seuil de la porte.

WARREN KUMARI: En Virginie, on n'a jamais de séisme, alors nous partons tous à la course.

PAUL HOFFMAN: Bien, nous nous mettons sous le seuil de la porte.

Merci. Je vais vous montrer une autre diapo liée à la révocation.

Je ne sais pas comment je vais continuer après un Séisme, mais bon. En Californie, nous faisons un tout petit peu ce que disait Warren, nous paniquons et nous partons à la course.

Bon, après la révocation vous avez là un graphique qui vous montre la barre verte au milieu, c'est ce à quoi on s'attendrait après la révocation. Ceci montre le changement dans les taux de requête par adresses individuelles. La bande verte montre la racine qui demande DNSKEY à la même vitesse. Mais il y a beaucoup d'hébergeurs qui demandent la DNSKEY qui ne la demandait pas auparavant. Donc quelque chose de la révocation a fait que de nouveaux hébergeurs, enfin des hébergeurs qui n'étaient pas là avant, aient commencé à demander davantage. C'est pour ça qu'ils étaient dans la partie supérieure.

Et les gens ont des théories à cet égard. Il y a certains chercheurs qui travaillent sur cela, mais c'est un autre exemple de ce que nous avons appris grâce au recueil de données que l'on a pu avoir pendant le roulement de la KSK. Et cela signifie que nous ne savons pas autant de choses que nous le croyons. 7

Voyons ce que disent les gens à cet égard, et nous allons ensuite voir ce que vous avez à dire. Voilà un choix aléatoire de ce que les gens ont dit sur cette liste de diffusion et dans des réunions préalables.

Pourquoi est-ce qu'on fait le roulement pour commencer ? Quelles sont les motivations. Pour bon nombre, il y a une réponse qui est évidente, pour d'autres la réponse est différente. Et il s'agit d'un point de départ de l'analyse, qui est assez logique. Pourquoi le roulement se fait-il ? Pour commencer. Si on a décidé de le faire, pourquoi ? À quelle fréquence, toutes les X années ? Et ce chiffre X peut représenter différents chiffres selon la personne. Ou faire le roulement quand ce sera nécessaire, ou bien nous ferons le roulement, mais il faut attendre que cela soit nécessaire. I

Il y en a qui disent que nous en sommes encore à un niveau de sécurité pertinent, nous devons le faire quand nous aurons les outils appropriés. Donc nous ne saurons pas quand ils seront à un niveau approprié, parce que les outils ne seront jamais suffisamment bons.

Il y a des gens qui disent qu'on a un meilleur « bootstrapping » pour le résolveur, pour que ceux qui sont aujourd'hui soient sûrs d'avoir la clef. Et il y en a qui disent que ce nécessaire, qu'il n'y a pratiquement pas de dommages ultérieurs visibles. Alors ce serait bien que les gens disent que l'on peut mettre cela à jour. Mais le plus probable est que l'on décide de quelque chose intermédiaire.

Est-ce qu'il faut avoir des clefs standby ? À l'heure actuelle, il y a deux clefs de l'ensemble des clefs de la racine. Même s'il y a un mois que l'on a une seule clef, qui est la nouvelle. Est-ce qu'il faut avoir des clés, des nouvelles clefs ou des clefs de réserve ou des clefs standby… tout cela se rapporte… Le nom de cette séance c'est le futur des KSK. Donc est-ce que nous devons avoir des clefs de réserve ? Est-ce que l'ensemble des clefs doit être plus grand ?

Il y en a qui parlent, qui demandent si nous devrions modifier l'algorithme de signature dans le prochain roulement. Et, encore une fois, quelles sont les considérations les plus importantes dans ce cas-là ? Tout le monde n'est pas prêt pour un changement d'algorithme, qui pourrait être utile, mais qui pourrait avoir des effets collatéraux, dont certains pourraient être dangereux.

Toutes ces choses-là, c'est des choses que nous pouvons aborder aujourd'hui, des thèmes que nous pouvons discuter aujourd'hui. Donc parlons-en.

Nous avons un micro disponible pour ceux qui ne sont pas assis autour de la table, pour ceux qui sont au tour de la table levez la main. Kathy et moi choisirons… Non Russ le fera. Je vais me mettre un petit peu comme ça pour pouvoir voir.

Ce n'est pas parce que je viens de la Californie et que j'aille vers la porte… Comme ça je peux vois ceux qui lèvent la main.

Donc soyez créatifs, parlez de choses nouvelles. Vous n'êtes pas obligé de répéter ce que d'autres auront dit. Pensez à la manière dont ce que vous allez dire va avoir un effet sur ce qu'il se passe.

La dernière que nous voulons avoir à faire, c'est un changement dans le DNSSEC qui provoque la crainte des gens. Si nous voulons faire des changements, c'est que nous voulons le faire pour que les gens aient une confiance accrue, qu'ils sentent qu'ils sont sur un système plus stable.

Bon, c'est la dernière fois que je parle et je le fais pour dire ce qui suit : ce que vous direz maintenant, je vous prie de l'envoyer s'il vous plait dans la liste de diffusion.

Je n'ai plus de diapo, donc ne vous sentez pas du tout limité, en aucune mesure.

Qui veut commencer ? Sauf Warren.

RUSS MUNDY: Nous vous demandons de vous présenter avant de commencer votre allocution.

PAUL HOFFMAN: Bon, je crois que j'ai réussi à vous faire peur.

WARREN KUMARI: Bon, je vais faire peur à tout le monde aussi.

On parle de la question de ces clefs de réserve, ou accessoires. Alors, le plan était toujours d'avoir une clef de réserve. Standby Key en anglais. Si on avait eu cette clef de réserve, les futurs changements de clef n'auraient pas créé de la crainte, parce que cette clef de réserve aurait toujours été là.

Alors il faut comprendre comment fonctionne le système, et nous devons pouvoir anticiper ce qui va se passer quand il y a un changement à faire.

En ce moment, on n'a pas cette connaissance.

PAUL HOFFMAN: Je crois que vous entrez en contradiction. Vous trouvez que la clef de réserve est une bonne idée, comme vous l'avez dit à la fin de votre commentaire ?

WARREN KUMARI: Je crois que ce serait bien de faire des tests des clefs de réserve. Je crois que ce serait une bonne idée de la voir. Il faut la mettre en place, mais aussi je dois évaluer ceci par rapport au fait que si on fait quelque chose sur le DNSSEC, on a toujours une surprise.

Alors il faut que l'on ait une clef de réserver, mais il faut mieux connaitre la question.

PAUL HOFFMAN: Yoshiro.

YOSHIRO YONEYA: Je suis du JPRS. Moi je suis pour le roulement de la KSK, et de l'avoir remis un peu à plus tard, parce qu'avec cette expérience, on a pu mieux comprendre la situation et les opérations veulent justement avoir une opération plus stable.

Ce type d'événement doit être planifié, et il faut le faire dans le temps nécessaire pour voir comment le mettre en place et comment répondre.

Je suis donc d'accord avec le roulement.

PAUL HOFFMAN: Merci. Je dois vous dire, vous avez un délai ? Vous pensez à un délai ?

YOSHIRO YONEYA: Je crois que la fréquence est importante. Je crois qu'une fois tous les deux ou trois ans, ce serait une fréquence acceptable. Moins de 5 ans.

PAUL HOFFMAN: Moins de 5 ans, mais avec une certaine continuité ou régularité, n'est-ce pas ? Merci.

NON IDENTIFIE: Bonjour, je suis le représentant du .[DECA] du Danemark. Je suis d'accord avec le roulement fait de manière régulière.

Avant de voir ces graphiques, je dirais qu'il faut le faire avant un délai de 5 ans. Mais maintenant, j'ai des doutes sur la fréquence. Je ne suis pas si sûr que ça, par rapport à la fréquence.

On devrait pouvoir décider le délai pour faire les changements, ainsi que pour vous de décider le changement de la clef pour la première fois, parce qu'on ne savait pas ce qui allait arriver.

Je crois qu'il faut faire le roulement, avec une plus grande fréquence. Je suis d'accord avec Warren, même si, vous vous en doutez, je suis d'accord avec lui du fait qu'il faut faire des tests. Au Danemark, on n'a plus de clef de réserve.

PAUL HOFFMAN: Ha, je vous demande, racontez-nous, parce que c'est la première fois que j'entends quelque chose de la sorte. Vous pouvez nous en parler ?

NON IDENTIFIE: Bon, je vais parler pendant quelques instants. Cette clef de réserve, qu'est-ce qu'elle évite ? Qu'est-ce qu'on essaye de

résoudre en ayant cette clef de réserve ? Quels sont les scénarios possibles ?

Dans notre cas, nos clefs privées, que ce soit les clefs en ligne ou les clefs de réserve de notre infrastructure, face à une menace d'infrastructure, et bien dans ce cas, on pourrait changer la clef. Si ceci va affecter notre clef de réserve, ça ne vaut pas la peine de l'avoir.

Nous avons donc pensé à une infrastructure différente ou séparée. Pour nous, c'est plus facile de créer une nouvelle clef et de faire la nouvelle signature avec cette nouvelle clef, au lieu d'avoir la clef de réserve.

C'est bien entendu beaucoup plus facile au premier niveau des noms de domaine.

PAUL HOFFMAN: Vous n'êtes pas dans la racine, mais vous êtes à un très haut niveau. Je reconnais vos efforts. Vous avez écrit quelque chose par rapport à cette décision ? Le document étant danois ?

NON IDENTIFIE: Je ne sais pas, je ne me souviens pas.

PAUL HOFFMAN: Vous pouvez nous dire ou voir s'il y a des documents? Ils seraient vraiment très utiles pour toute la communauté. Si vos organisations ont fait des enquêtes et ont écrit un document, même d'une page, et si ce document a été publié, ce serait vraiment bien de partager cette information. Et dans votre cas, même si l'information est en danois, je connais même un traducteur professionnel en danois.

NON IDENTIFIE: Ok, on va le faire.

PAUL HOFFMAN: Ou même si les personnes qui ont pris cette décision sont à même d'écrire sur la question, ce serait très utile pour ce genre de débats. Merci beaucoup.

J'évite de donner la parole à Warren, parce que je veux inviter tous les autres participants à faire des commentaires.

JACQUES LATOUR: Dans le contexte de l'ICANN, je voudrais savoir quel est l'avantage d'avoir plus d'un HSM, un module de logiciel de sécurité.

PAUL HOFFMAN: Nous avons, dans le groupe de cryptographie de l'IANA, de très bons professionnels qui décident s'il faut prendre ou pas la

décision. Si la communauté veut avoir une clef de réserve, ces experts de l'IANA vont certainement penser à une proposition qui sera présentée à la communauté.

Voyons voir… Combien de personnes ici dans la salle, représentent des ccTLD et des gTLD ? Et de ces personnes qui ont levé la main, combien ont une KSK de réserve ?

WARREN KUMARI : Merci, je me demandais si c'était une clef de réserve publique ou non publique.

PAUL HOFFMAN: Peu importe, une clef de réserve. Combien parmi vous ont une clef de réserve ?

J'espérais voir plus de mains levées.

Alors je vais vous demander d'écrire cela. Warren, vous aussi levez la main. Écrivez cette situation, cette expérience.

Nous on parle d'algorithmes, de changements d'algorithmes faits par certains ccTLD, les résultats sont différents. C'est vraiment très utile de préparer des documents écrits sur la question.

Warren, je vous passe la parole.

WARREN KUMARI: Ça dépend de l'objectif de la clef de réserve. Si on veut cette clef pour qu'une clef soit disponible en cas de défaillance de la clef principale, alors dans ce cas il faut penser à une conception différente. Différente du cas où on aurait besoin d'une clef de réserve pour faire le roulement de la KSK.

Si on a toujours deux clefs publiées, et si on en change une et on enlève l'autre, c'est bien plus facile. Ceci facilite le mécanisme.

JACQUES LATOUR: Je crois qu'il y a une clef de réserve qui serait une clef publique.

[Deux orateurs qui se superposent]

WARREN KUMARI: Alors, dans ce cas, la révocation n'est pas un événement si important, et on pourrait avoir une clef de réserve pour faire un changement en cas d'urgence.

Je sais qu'il faut continuer à aborder la question.

PAUL HOFFMAN: On pourrait continuer à traiter de la question dans notre liste de diffusion.

WARREN KUMARI: Pour ce qui est de votre question par rapport à la fréquence du changement de clef, il y en avait qui voulaient faire des changements annuels, ou même plus fréquents. Je crois que les données les plus récentes sur cette question, et bien il faudrait analyser les causes, bien étudier les cas, voir quels ont été les problèmes qui se sont présentés.

Et lors du prochain roulement il devrait y avoir moins de problèmes pour que la fréquence de changement de clefs soit établie, une fois par an.

Ce serait mieux, mais il faut continuer de débattre de la question dans notre liste de diffusion.

PAUL HOFFMAN: Vous parlez de ce que pensent d'autres personnes, qu'en pensez-vous ?

WARREN KUMARI: Je savais que vous alliez me poser cette question. Pour moi, le roulement devrait être annuel ou même tous les 6 mois.

PAUL HOFFMAN: Et maintenant qu'en pensez-vous ?

WARREN KUMARI: Maintenant, je ne peux pas vous répondre jusqu'à ce que l'on ait résolu cette question en particulier, ce problème en particulier. Et alors, dans ce cas, on aura de meilleures informations sur le risque, savoir s'il est structurel, s'il a trait à la mise en œuvre ou à d'autres facteurs. Dès que nous aurons la réponse, on pourra prendre une meilleure décision.

PAUL HOFFMAN: Si personne d'autre ne demande la parole, je continue à parler à Warren. Vous avez dit : une fois que l'on trouvera une solution à ce problème. Il y a une ligne dans les 4000, si ce niveau est maintenu constant pendant 4 ans, on a trouvé une solution au problème ou pas ?

WARREN KUMARI: Ceci s'est passé après la révocation. Mais le problème apparait au moment de la révocation et ce qui se passe après.

PAUL HOFFMAN: Je vois qu'il y a quelqu'un qui demande la parole, allez-y s'il vous plait.

NON IDENTIFIE: Bonjour, je m'appelle [inaudible], je représente un registre, .OE. Je me demande, que se passerait-il si on revenait à la KSK

précédente ? Peut-être la situation serait normalisée ? Je sais bien que c'est tard pour cela…

PAUL HOFFMAN: Une fois que la clef est révoquée, même pour 5 secondes, on ne peut plus revenir en arrière, parce que sinon les gens n'auront plus confiance à cette clef. À ce moment-là, personne ne nous a demandé de revenir à la clef précédente.

Je vais vous montrer encore une fois le graphique. Dans cette deuxième ligne des 4 000, il y a quelque chose d'intéressant. Personne n'a pu m'expliquer pourquoi ceci se passe pendant plus de 48 h après la deuxième barre rouge. Et même dans ce cas, être un résolveur de validation qui répond à des consultations, dans ce cas, je n'ai pas l'ensemble de clefs de DNS que je veux. Alors, c'est un indice nous disant qu'il y a un grand nombre de résolveurs sans que personne n'envoie une consultation, ou c'est quelque chose de plus mystérieux encore.

[TIM]: Tim au micro.

PAUL HOFFMAN: Excusez-moi, je ne vous avais pas vu.

[TIM]: J'ai pris note de ce que vous avez dit. J'aimerais voir un autre roulement de clef dans un futur pas très lointain, parce que je suis un scientifique, je fais des investigations, et je voudrais avoir des données.

Pour moi, ce type d'activités a trait à la clef précédente. À mon avis, ce niveau n'augmenterait pas au cas d'un autre roulement. C'est ma théorie personnelle.

Et pour ce qui est de la clef de réserve, moi je l'utilise pour un autre processus dans un HSM séparé, un module de logiciel séparé. Et ce que nous faisons, c'est utiliser la clef 6 fois, passer à une autre clef, mettre à jour la clef que nous avons utilisée et la laisser comme clef de réserve pendant 6 mois. Nous avons donc deux clefs disponibles tout le temps.

PAUL HOFFMAN: Merci. Jaap ?

JAAP AKKERHUIS: Il faudrait voir pourquoi ceci arrive. Il y a des résolveurs qui ne font vraiment aucune validation. Alors, on dirait que ceci est utilisé en aveugle. Et on essaye de faire la validation de toute manière.

Le changement de [inaudible] va toujours affecter la façon de travailler avec les clefs. De toute manière, il faut voir d'où viennent ces activités, qui les fait et pourquoi.

PAUL HOFFMAN: Si vous avez raison, alors en 20 secondes la courbe devrait diminuer.

JAAP AKKERHUIS: Bon, il faudrait le voir. Il y a beaucoup de gens qui utilisent des bibliothèques BIND de manière inattendue, et ceci pourrait être la cause de ce comportement.

PAUL HOFFMAN: Peut-être quelques-uns parmi vous pourraient être au courant du roulement de clef le 11 octobre 2017. Il y a eu beaucoup de résultats présentant des anomalies, voilà pourquoi on a remis le roulement à plus tard. On a vu des données, des chiffres, et nous avons découvert que certaines applications utilisaient cette bibliothèque de manière incorrecte.

Nous avons pu communiquer avec ces développeurs de logiciels qui nous ont dit : ha, je ne m'étais pas rendu compte. Et ils ont trouvé une solution au problème.

Et lors de la mise en œuvre, nous avons vu une diminution des anomalies.

Tout cela est possible, mais on ne peut pas calculer let temps.

Vous voulez poser des questions ? Faire des commentaires ?

NON IDENTIFIE: Lorsqu'il y a des clients spécifiques qui ont ce comportement récurrent, on pourrait peut-être avoir un algorithme pour aborder la situation avec ce groupe de clients en particulier. C'est un commentaire plutôt.

WARREN KUMARI: Oui, il y a des serveurs qui en fait mettent en place des technologies qui permettraient de limiter ce type de conduite et de réitération de consultation. Il semblerait que ces pratiques ne soient pas respectées par ces clients, et que cela ne fonctionne pas bien.

Ce que l'on pourrait mettre en œuvre, c'est de voir la vitesse des consultations, et voir si une réponse erronée déclenche une nouvelle consultation, ou voir ce qu'il se passe dans ce cas-là, pour voir quel est le comportement.

Voilà, ce serait une expérience intéressante vraiment. Mais bon. Oui, ce serait peut-être une bonne idée d'établir une limite. Vous

pouvez faire en sorte de répondre à ces consultations pour que le reste des consultations soient plus lentes.

PAUL HOFFMAN: Mais on ne le sait pas. D'autres commentaires ? D'autres questions ?

JACQUES LATOUR: A mon avis, ces données sont des données de botnet, c'est-à-dire ces données viennent de sources qui ne sont pas claires ou licites. Alors si tout s'agissait d'une défaillance des serveurs, les gens se plaindraient et on en trouverait une solution. Je ne crois pas qu'il y ait des personnes inactives pendant une semaine ou un an, ou quoi que ce soit.

Alors c'est comme faire du bruit, disons, sur internet. Je ne vois pas que ce soit un problème très grave. On a des informations disponibles, mais je ne crois pas que ce soit si important par rapport au roulement de la clef.

Les API, les outils de production, fonctionnent bien. Parce que s'il y avait eu des défaillances, ces défaillances auraient été réglées.

Ce sont des données intéressantes, il peut y avoir d'autres données intéressantes, on pourrait trouver des réponses à des situations déterminées. Alors, par exemple, notre domaine .CA,

pendant 5 minutes, on a des pics d'activités qui font du bruit au niveau du réseau. Mais ce n'est pas grave, parce que s'il y avait une défaillance du système, les utilisateurs l'auraient informé, ils auraient présenté des plaintes.

Par exemple, le pense au roulement de la clef tous les 6 mois, il faut bien le faire. Si on va utiliser le DNSSEC, il faut démontrer qu'on n'a pas peur. Et dans un an ou deux, il faudra faire le roulement une fois que l'on sera à l'aise, que nous serons confiants que nous pouvons faire le roulement avec une certaine régularité.

Pour ce qui est des consultations, par exemple, Andrei peut vouloir écrire un code pour embêter tout le monde.

PAUL HOFFMAN: Nous avons donc un ensemble d'opinions, de questions.

RUSS MUNDY: Bien, dans l'une des présentations que nous avons eues avant le déjeuner, il y a eu une révision du trafic, et Wes nous a présenté une perspective. Les analyses n'étaient pas exactement identiques, mais elles étaient semblables. Dans l'analyse de Duane, on a eu ce souci que le taux de croissance augmente après la révocation.

Cet accroissement peut être lié à la révocation ou pas, mais cette incidence du timing nous fait savoir qu'il y a quelque chose de pas tout à fait fiable, disons, en quelque sorte.

Si ceci a changé le 22, quand on a révoqué la clef, que la vitesse de croissance n'a pas été modifiée, il faut que nous voyions pourquoi.

À mon avis, nous devons commencer à considérer à quel moment nous pourrions commencer à rendre cet événement régulier. Les gens pensent qu'il y a d'autres questions.

PAUL HOFFMAN: En fait, je ne vous poussais pas à dire votre opinion, mais je vous demande quand même de l'exprimer.

RUSS MUNDY: Ce que je vous disais, c'est que nous devons essayer de faire un roulement de la KSK une fois par an. Cela permet de faire les choses de telle manière que l'on puisse résoudre les problèmes qui se posent, mais c'est une période suffisamment courte pour que les gens puissent s'y faire et répondre à une certaine cadence du roulement. Je crois que nous devrions viser cela, mais pas avant d'avoir su ce qu'il se passe avec certaines spécifications de données que nous avons jusqu'ici.

Réfléchissez-y et voyons comment nous pourrions faire pour avoir une périodicité d'un an.

PAUL HOFFMAN: Jaap et Andrei travaillent tous les deux pour des entreprises qui distribuent les codes des résolveurs. Russ dit une fois par an. Vous deux, comme vous avez des clients qui dépendent de vous, des clients qui se servent de votre logiciel, ou qui ne dépendent pas beaucoup de vous mais qui se servent de ce logiciel, que pensez-vous de cette fréquence annuelle ?

[ANDREI]: Je n'ai pas d'opinion ferme à cet égard. C'est beaucoup plus compliqué, la validation avec DNSSEC est beaucoup plus compliquée. L'utilisateur final, l'équipement pour l'installation du client, enfin la gestion de la validation là est beaucoup plus difficile. Et il y a la question du bootstrapping et du routeur. Donc tout faire à un moment est difficile.

En tant que technicien, expert technicien, je soutiens la position de Russ, mais en tant que fournisseur d'ISP, c'est beaucoup plus difficile.

JAAP AKKERHUIS: Moi, je suis d'accord en ce sens que nous devons faire cela fréquemment. Je n'ai pas encore défini cette fréquence, mais nous devrions attendre jusqu'à ce que nous ayons un panorama plus clair, pour savoir quels sont nos besoins.

Il faut permettre aux gens de s'y habituer. Les logiciels sont mis à jour bien des fois, plus d'une fois par an, non ?

PAUL HOFFMAN: Vicky?

VICKY RISK: Oui, bien sûr, nous mettons à jour notre logiciel plus d'une fois par an. Et nous avons un logiciel qui est stable.

La version de [BIND], telle qu'elle a été présentée pendant une présentation précédente, il y a des gens qui continuent à travailler avec des codes datant de 6 ou 7 ans.

Je n'ai pas de solution, mais si j'en avais une, je m'en servirais tout de suite. Je crois que c'est bien de le faire régulièrement.

Bien sûr pour nous, c'est beaucoup de travail supplémentaire, et j'imagine publieurs de codes ouverts c'est la même chose, parce que nous faisons beaucoup de vérifications, nous développons de nouveaux essais et de nouveaux tests. Enfin, nous donnons une solution à des problèmes différends, nous mettons en œuvre

des options de télémétrie différentes pour voir les résolveurs et les Key tags. Cela devrait être beaucoup plus facile la prochaine fois.

J'aimerais bien pouvoir d'abord comprendre ce qu'il se passe par rapport à ces comportements bizarres, parce que pour moi, à un moment donné, il doit y avoir un bug, une défaillance.

PAUL HOFFMAN: Je ne sais pas s'il y en a d'autres dans la salle que je ne connais pas ou que je ne vois pas. Je ne sais pas s'il y a quelqu'un d'autre.

STEVEN CARR: Steven Carr de [Infoblox]. Nous sommes dans une position intermédiaire, disons. Nous ne donnons pas notre soutien à la [5011], je sais que c'est une question, c'est tout un paquet.

PAUL HOFFMAN: Et maintenant c'est beaucoup plus important encore ce thème.

STEVEN CARR: Moi, j'aimerais bien – pour des raisons très égoïstes – de rouler cela une fois par an. Donc en ce sens là, je donnerais mon soutien à la RFC 501, pour que les utilisateurs n'aient pas cette charge supplémentaire pour pousser la racine sur un seul espace.

Je recommande que les zones soient établies une fois par an. C'est la norme que nous avons pour notre système.

Nous avons pris cette décision sur la même base, à peu près, que l'on montre ici. Il faut que ce soit fait avec une fréquence régulière, que les gens n'oublient pas la manière de le faire, et qu'il y ait cette idée que les choses bougent. Si c'est plus long qu'un an, la situation sera telle que les gens changent d'emploi, quittent l'industrie, il y a des gens… Et cette personne n'est plus familière de ce qui doit se passer parce que cela s'est fait, il y a trois ans, de la même manière.

Donc il faut que ce soit fait une fois par an. Et pour une question de pression, cela va se trouver dans la pensée des gens.

PAUL HOFFMAN: Vittorio voudrait parler de la fréquence.

VITTORIO BERTOLA: Je voudrais discuter de cela avec les gens de [PowersDNS]..

PAUL HOFFMAN: Embêtez-les suffisamment pour qu'ils participent à la liste de diffusion. Voilà, j'essayais de parler avec les développeurs de logiciels.

Nous avons encore quelques minutes, et je voudrais éviter, dans la mesure du possible, que Warren ne parle encore. Même si je l'aime beaucoup, je voudrais qu'il y ait d'autres personnes qui s'expriment, des gens qui n'auront pas pris la parole encore. Voilà, des gens qui sont là, au fond de la salle. Voilà.

AKIRA KATO: Je suis le représentant du WIDE Project.

Il s'agit d'un changement intéressant. La taille du paquet, dans certains cas l'algorithme de données doit être soutenu par tous. Il faut pouvoir annoncer, il est essentiel d'annoncer, que le roulement se fera par exemple en 2025, et que l'on aide les gens à s'y préparer.

Je pense qu'il faut faire une annonce à cet égard.

Est-ce que je peux faire une annonce sur le séisme ? Le séisme s'est produit à plus de 100 km de profondeur. Ne vous inquiétez pas, il n'y aura pas de tsunami.

Mais, si vous êtes près de la côte et que vous sentez un séisme très fort, ce que vous devez faire, c'est monter à l'étage le plus élevé du bâtiment où vous êtes.

PAUL HOFFMAN: J'ai un ami qui a vécu et qui a survécu à un tsunami, donc je vous recommande de bien vouloir suivre ce conseil-là.

Bien, je crois que c'est un thème intéressant, peut-être moins intéressant que la KSK hein…

FREDERICO NEVES: Je m'appelle Frederico de .BR. Un autre commentaire sur le roulement.

À partir de l'histoire, que nous avons eue, il n'y a eu qu'un roulement de la clef, qui a pris plusieurs années. Donc le fait de penser à un changement d'algorithme, ça prendra plus d'un an.

Alors, nous ne devrions peut-être pas aborder ce sujet maintenant, même si je reconnais qu'il faudrait faire cela. Parce qu'il est fort probable que la taille du paquet ne sera pas un problème d'ici 10 ans. Nous aurons probablement des transports différents qui dépasseront cette question.

C'est juste un commentaire.

PAUL HOFFMAN: Comme nous n'avons plus de temps, je veux vous remercier tous de vos commentaires et je vous encourage vivement à participer dans cette adresse URL et à participer à la liste de diffusion.

Ce qui est le plus important, si vous avez dit aujourd'hui quelque chose, veuillez le répéter sur la liste de diffusion. Si vous êtes dans une organisation où ce thème a de l'importance, même si vous n'avez pas d'opinion, même si l'organisation n'a qu'une faible opinion, même si c'est une opinion qui n'est pas officielle, ne vous empêchez pas de le mettre sur la liste, parce que ce sera important pour tous ceux qui font des recherches, et même pour ceux qui font de la recherche informelle ou qui se mettent à supposer ce que signifie le graphique, ou quel sera le graphique du 23 ou du 24 mars. Si l'on tient compte du TTL de la durée de vie.

NIC.BR a fait une très bonne analyse, soit dit en passant, du changement d'algorithme. Je crois que les gens de CZ.NIC ont dit cela, je crois. Donc tous ceux qui auront une opinion et qui auront réfléchi sur ces sujets, n'oubliez pas de partager votre opinion, parce qu'elle est vraiment importante.

Bien sûr ce sera l'IANA qui prendra la décision de la manière dont on avancera dans l'avenir. C'est l'organisation de l'ICANN qui va recueillir les déclarations sur l'URL et la publiera sur la page pour que l'on puisse trouver cela plus facilement.

Nous espérons bien pouvoir avoir davantage de choses de votre part. Voilà, c'est tout.

RUSS MUNDY: Merci beaucoup Paul, et tous les autres, de vos présentations d'aujourd'hui. Et merci d'être ici pour cette dernière partie de la séance.

C'est une séance de questions/réponses. Il y a un certain temps qu'on ne le faisait pas. C'était une idée du comité du programme que de demander des questions, des observations, des remarques, des opinions sur le programme que nous avons maintenant et de celui que vous aimeriez avoir pour la prochaine réunion. Parce que nous attendons toujours l'avis de la communauté, savoir que cela est utile pour la communauté, par rapport à tout thème lié à la question du DNSSEC.

C'est pourquoi je vous demande donc de prendre la parole pour donner vos opinions, aussi bien sur ce que vous avez entendu dire aujourd'hui, que sur ce que vous aimeriez entendre pour le prochain atelier.

Personne ? Bon ne parlez pas tous ensemble, c'est assourdissant.

Yoshiro ?

YOSHIRO YONEYA: Est-ce que je pourrais parler japonais ? Parce qu'il y a beaucoup de japonais ici.

[Les interprètes s'excusent, Yoshiro parle japonais, ce n'est pas ma langue de travail]

Si nous avions une interprétation du japonais, cela aurait été beaucoup plus simple pour nous que de pouvoir participer.

[L'orateur continue à parler japonais]

NON IDENTIFIE: C'est la première fois que je suis dans une réunion internationale. Ce thème de discussion a un caractère fortement professionnel, cela dépend des thèmes. Il y en a qui sont plus difficiles. Alors s'il y avait une interprétation disponible du japonais, il y aurait davantage de Japonais qui assisteraient à des réunions de ce type.

Voilà, c'est mon avis.

RUSS MUNDY: En ce qui concerne cette remarque, j'aimerais bien demander aux personnes présentes. Je vois qu'il y en a qui se sont servi du service justement d'interprétation simultanée. Est-ce qu'il y en a parmi vous qui ont des commentaires sur l'utilité du service, ceux qui se sont servis du service d'interprétation aujourd'hui. J'ai vu qu'il y avait une personne qui s'en servait auparavant, mais je ne vois pas maintenant qu'il lève la main. Mais je veux remercier nos interprètes, parce qu'elles font un travail fantastique.

Nous avons encore le temps pour d'autres commentaires. Je ne sais pas si…

VITTORIO BERTOLA: Mon seul commentaire c'est que je comprends pourquoi il y a le français et l'espagnol, mais ce serait bien aussi d'avoir les langues locales, au moins du lieu où l'on est, qu'il n'y ait pas seulement l'anglais.

RUSS MUNDY: Est-ce qu'il y a d'autres commentaires ? D'autres commentaires ou d'autres questions des participants ?

Nous avons quelques membres du panel encore, et il y en a qui sont déjà partis. Si quelqu'un veut faire des commentaires ou poser des questions plus tard… Il y en a qui sont ici avec nous. Donc n'hésitez pas à poser les questions que vous voudrez poser.

Bien, pour le prochain atelier, prochain séminaire, est-ce qu'il y a des commentaires des personnes ici présentes ?

Voilà je demande : à votre avis, quel est le résultat le plus utile de toutes les présentations que nous avons eues ? Lequel des résultats a été le plus utile, qu'est-ce que vous aimeriez voir la prochaine fois ?

Qui veut faire des commentaires à cet égard ?

NON IDENTIFIE: C'est un commentaire de nature générale. Ne le prenez pas comme une critique à l'organisation de l'ICANN. Il a été vraiment très, très difficile d'organiser toutes ces séances ce matin. Il y a eu plusieurs séances sur la sécurité, sur la lutte contre l'utilisation malveillante et d'autres questions liées à la sécurité qui se produisaient en même temps. Je sais qu'il n'est pas possible d'organiser autant de séances.

Encore une fois, je demande de faire un effort pour qu'il n'y ait pas de séances en simultanée.

RUSS MUNDY: Oui, il y a eu beaucoup de difficultés, surtout pour le personnel technique. Nous prenons note de votre remarque. Nous allons essayer d'améliorer cet aspect. Mais c'est bon d'avoir vos commentaires. C'était quelque chose que nous avions imaginé, mais c'est bon que tout le monde le sache.

Un autre commentaire ?

[JOHN]: Moi, j'ai aimé ce que l'on a appelé la restriction de la participation de Warren. Historiquement, la plupart des présentations étaient très techniques. Voilà ce que nous faisons pour le DNSSEC dans

les registres, comment nous faisons-le [inaudible] des résolveurs. Donc il faudrait travailler à un niveau plus général des thèmes. Il faudrait essayer d'aborder les problèmes.

Bien sûr, il y a une limite, il y a un moment où l'on est à court de thèmes intéressants, mais c'est intéressant pour la préparation de l'ordre du jour, ou de l'agenda pour l'avenir.

VITTORIO: Il y a beaucoup de choses sur le navigateur. On va continuer cette discussion à Marrakech, cette discussion sur les régulateurs. Pas la politique objective, mais la politique humaine.

JOHN: Je ne sais pas comment on fait la résolution. Nous savons qui fait la résolution dans les navigateurs, mais s'il y a un membre du monde académique qui aurait déjà étudié la question, ce serait intéressant de le savoir.

RUSS MUNDY: Est-ce qu'il y a d'autres commentaires ou questions ?

VICKY RISK: J'ai beaucoup aimé toutes les présentations, et en particulier les spécialisations sont très intéressantes. Mais bien que les gens qui verront les fichiers en ligne ne puissent pas voir les animations.

J'ai apprécié qu'on nous ait montrés des données qui n'ont pas été analysées. C'est bien de savoir qu'il y a des problèmes qui ne sont pas résolus. C'est mieux que d'avoir seulement les réponses à ces problèmes. Je crois que c'est très utile.

Et j'aime bien que dans ces séances, pendant ces séances, les gens partagent leur expérience opérationnelle. J'ai apprécié la présentation de .AU en particulier. Chaque fois que quelqu'un essaie de transférer des zones il y a des problèmes qui se présentent.

Voilà donc les deux points pour lesquels je voulais exprimer ma reconnaissance. J'aime aussi cette présentation de haut niveau, pour savoir à qui l'utilisateur final doit faire confiance. Dans ces domaines nous n'avons pas parlé de la capacité d'utilisation ou de recherche des utilisateurs finaux. C'est quelque chose que nous avons laissé de côté, et nous avons profité du fait qu'il y a beaucoup de gens qui s'occupent de politiques.

RUSS MUNDY: Bien. Vous dites que vous avez apprécié la présentation de ces données, même si ces données n'ont pas été peaufinées, terminées. Est-ce que vous aimeriez voir davantage de choses de ce type, des choses qui ne sont pas terminées ?

VICKY RISK: Oui, oui, bien sûr, ça me donne du travail, c'est du travail que j'aurais à faire, je pourrais prendre ça pour mon retour, et je pourrais l'analyser, je pourrais comparer à nos propres données.

J'aimerais bien pouvoir faire un tout petit peu plus de recherches. Ceci pourrait expliquer une partie du trafic.

Par rapport à la question de Warren, pourquoi l'URL n'est pas plein de commentaires, cela m'a fait réfléchir, et j'ai pensé à faire un suivi.

RUSS MUNDY: Bien, très bien, nous prenons bonne note de vos commentaires. Quelles autres suggestions avez-vous à faire pour notre prochain atelier du DNSSEC ? Est-ce que vous avez des suggestions pour le comité d'organisation ou des thèmes que nous n'aurions pas abordés par exemple ?

JACQUES LATOUR: Nous voulions ajouter des thèmes de sécurité, d'hier. Nous voudrions également faire moins de ce type de débats ou ces panels, on voudrait voir des questions relatives à la sécurité, et on aimerait voir ce qui vous intéresse par rapport à la sécurité.

VICKY RISK: On a mentionné la question de la superposition avec d'autres questions techniques ou relatives à la sécurité. Je ne sais pas si cela est possible.

BARRY LEIBA: Vous l'avez peut-être fait, je ne sais pas si c'est possible ou pas, mais peut-être pourrait-on contacter des opérateurs importants qui n'aient pas mis en place DNSSEC et qu'ils nous expliquent pourquoi ils ne l'ont pas fait.

RUSS MUNDY: Ça fait quelques années que l'on ne fait pas. Il y a du temps qui s'est écoulé, et on a la nouvelle KSK, donc il n'y a plus d'excuses disons.

JACQUES LATOUR: On pourrait le faire au Canada, à Montréal. Parce que là, il y a presque tous les ISP qui n'ont pas mis en place le DNSSEC, et ils sont locaux.

NON IDENTIFIE: Nous avons déjà parlé à d'autres participants. Il y en a beaucoup dans cet écosystème, non seulement les acteurs du DNS mais les opérateurs de registre et bureaux d'enregistrement. Il faut parler de la sécurité du DNS par opposition au DNSSEC.

RUSS MUNDY: Parfait. Alors ceci est cohérent avec débats que l'on a menés au comité d'organisation de cet atelier, pour inclure des questions au-delà des aspects centraux des DNSSEC, et les inclure dans cet atelier. Peut-être même un jour cet atelier changera son nom. Alors définitivement, oui, on veut élargir les thèmes à aborder.

Ceci dit, j'aimerais passer à la question suivante qui nous intéresse au cours de cette séance. Nous, on a un comité d'organisation et nous recevons du matériel, des documents de la communauté. Nous aimerions donc recevoir des réponses, des commentaires, à notre convocation, pour la présentation de documents, de matériels pour ces séances.

Vous avez l'opportunité de nous raconter quelles sont les questions que vous voudriez aborder, et nous présenter, qui seraient à votre avis serait intéressant pour la communauté. Cette séance est pensée en fonction de la communauté. Alors, soyez alertes aux convocations de participation.

La prochaine réunion n'est pas si loin, c'est une réunion qui aura lieu vers la fin juin, je crois, du 23 juin…Bon fin juin. Alors, commencez à réfléchir.

BARRY: Où trouvons-nous la convocation ? Où sera-t-elle publiée ?

RUSS MUNDY: Nous l'enverrons à la liste principale de diffusion des participants des DNSSEC, je crois que c'est DNNSSEC.ORG.

JACQUES LATOUR: Nous l'avons aussi envoyé à la liste de diffusion de la communauté technique de l'ICANN pour les gTLD. En général, c'est l'un des courriers que les gens éliminent.

RUSS MUNDY: Si vous voulez faire des suggestions, si vous gérez l'utilisation d'autres listes de diffusion, n'hésitez pas à envoyer les contacts de ces listes aux organisateurs de cette réunion, et de cette séance.

Nous voulons savoir comment être utiles, comment pouvoir communiquer avec vous, les listes de diffusion, les plateformes de participation, etc. pour élargir la portée de nos communications.

Il y a quelqu'un dans la salle qui souhaite faire des commentaires sur la séance d'aujourd'hui ? Jacques ?

JACQUES LATOUR: On parle de l'enregistrement de DNSSEC au niveau des bureaux d'enregistrement. C'est-à-dire sortir cela de l'écosystème, et le

faire avec un opérateur de DNS, avec une clef CDS. Il faut voir comment faire, comment mettre en place cette mesure.

Nos bureaux d'enregistrement, et je parle au titre de ccTLD, en ce moment la plupart de nos bureaux d'enregistrement ne sont pas intéressés à la mise en œuvre de DNSSEC. Ce qui les intéresse c'est le DNS, mais pas la mise en place des DNSSEC. Alors si cela vous intéresse, vous pourrez aborder la question lors de la prochaine réunion.

RUSS MUNDY: Et bien, nous devrions donc recevoir ces suggestions dans notre convocation de participation. Nous prenons note de vos commentaires. Les membres du comité d'organisation de cet atelier.

Et maintenant, je voudrais faire une présentation. En général c'est la présentation de clôture pour cet atelier.

Cette présentation est adressée non seulement aux personnes ici présentes, mais aussi pour que toute cette documentation soit publiée en ligne. Alors, dès que vous voudrez chercher des ressources, avoir des documents de référence, savoir où aller pour trouver ce que vous voulez, pour mettre en œuvre le DNSSEC et améliorer votre sécurité, et bien là vous aurez toutes ces références, et tous ces documents.

Premièrement, il faut signer le TLD. Et ceci, d'après les derniers pourcentages, on ne le fait pas très bien. John, je ne sais pas si on a les pourcentages, on est à 85 ou 90 % du niveau de signature. C'est un très bon niveau, mais il faut l'améliorer encore. Alors, si vous n'avez pas encore signé, assurez-vous de signer votre TLD.

Si vous êtes un ccTLD, assurez-vous de travailler avec les bureaux d'enregistrement aussi. Pas mal de fois, les bureaux d'enregistrement trouvent des difficultés pour y participer.

Aujourd'hui, on ne voit que des statistiques. Et les statistiques nous informent mais jusqu'à une certaine mesure. Et même des fois, on ne les comprend même pas.

Tout opérateur de zone doit faire de même, signer sa zone, et vérifier que les bureaux d'enregistrement travaillent avec les DNSSEC, travaillent au sein de leur communauté.

Et nous avons besoin aussi de vos statistiques. L'OARC, nous recueillons et nous utilisons les statistiques dans ce centre d'opération et de recherches. Alors les statistiques sont toujours bienvenues pour apprendre en permanence.

L'entreprise pour laquelle on travaille, travaille avec une zone qui signe le DNSSEC, et je suis vraiment fier. Il faut offrir ceci à vos clients.

Les consommateurs doivent demander d'utiliser le DNSSEC. Un ISP ne travaille pas avec le DNSSEC, et il faut aussi valider, valider et valider.

Qu'est-ce que l'on peut faire ? On peut tous utiliser le DNSSEC. On peut aussi partager nos expériences, partager tout ce que l'on a appris avec d'autres membres de la communauté. Nous devons participer, présenter des commentaires, des opinions, partager des expériences.

Voici l'occasion pour moi, pour Jacques, pour Yoshiro et pour d'autres membres du comité d'organisation, de remercier tout spécialement les présentateurs, les orateurs, et les participants de cette journée de travail.

Il est également important de remercier nos sponsors du déjeuner d'aujourd'hui.

Merci beaucoup.

Je vous rappelle également que le SSAC et la Société Internet sont les entités qui organisent cet atelier.

Tout le monde aime voir ou trouver des choses sur le web. Voici quelques références. Il y a DNSSEC.ORG, et la liste de diffusion des DNSSEC. Et tout le monde est invité à participer à la prochaine conférence.

Merci beaucoup.

[FIN DE LA TRANSCRIPTION]