COPENHAGUE – Atelier sur les DNSSEC - 2e partie
Mercredi 15 mars 2017 – 11h00 à 12:45 CET
ICANN58 | Copenhague, Danemark

DAN YORK : ... qui s'appelle ComCast et nous avons Paul Ebersman qui est là pour nous présenter ce qu'ils sont en train de faire du côté de ComCast.

Paul, allez-y.

Pour ceux qui participent à distance, je précise que l'idée est d'avoir une discussion, donc on n'a pas nécessairement beaucoup de diapositives. On vous invite à participer et à poser des questions sur le chat, si cela vous intéresse. Kathy et Julie contrôleront la salle de chat et nous dirons si vous avez des questions. Je sais que nous avons des participants à distance.

Paul, pourriez-vous nous raconter ce que fait ComCast se préparer et comment vous collaborez avec d'autres FSI ?

[PAUL EBERSMAN] : Merci, Dan. Nous avons deux infrastructures que nous soutenons. 26 millions de foyers et trois ou quatre millions de PME. Nous avons également le secteur des entreprises de DNS et de TI. Nous faisons donc la validation pour tous ces utilisateurs.

Au moment où le roulement de clef se fera, nous aurons environ 300 serveurs récursifs de notre côté, en 50 et 60 serveurs du côté de l'Internet. On a décidé que même si on utilise des machines spécifiques pour des raisons de performance, on les considère comme des IDN. Tout est automatisé, on utilise des paquets et des paramètres selon le type de résolveurs.

Pour nous, l'automatisation n'était pas une méthode valable, tout comme le 5011, parce que ça entrait en conflit avec tous les serveurs qui faisaient le travail de push dont nous avions besoin.

Donc, ce que nous sommes en train de faire, c'est qu'on utilise la clef, on la valide, on fait des tests en ce moment, et on vérifie si tout fonctionne pour pouvoir passer à l'étape d'automatisation pour continuer à avancer à partir de ce moment-là. Une fois qu'on commence à travailler au laboratoire, on se sépare du reste.

Le plan, actuellement, est d'examiner si les entreprises utilisant des résolveurs et des machines ainsi que des AWS vont pouvoir s'adapter.

DAN YORK : C'est-à-dire que la nouvelle KSK va devoir fonctionner, autrement, au moment où on l'allumera, ça explosera ?

J'espère que vous avez ce que fait ComCast pour votre présentation de KSK.

PAUL EBERMAN : Oui, et c'est pour ça que je n'ai pas préparé de diapositive, Dan, ce n'était qu'une puce sur une diapo. Si ce n'était pas possible de résumer autant, ce ne serait pas faisable pour nous.

DAN YORK : Très bien, c'est compris.

Est-ce qu'il y a des questions pour ComCast au sujet de leur stratégie de roulement de la KSK ?

PAUL EBERMAN : C'était simple.

DAN YORK : Très bien. Maintenant, nous avons [Torbjörn] de [Interland].

[TORBJÖRN EKLÖV ?]: Bonjour. J'espère que vous comprendrez mon anglais. C'est [Torbjörn, Interland].

Je suis un peu fatigué, je me suis levé de très bonne heure, ce matin. Je m'appelle [Torbjörn], il faut m'appeler [Thomas].

Je me sens tout petit parce que je dois passer après ComCast, ce qui n'est pas évident.

Voici mon explication par rapport à ce que j'ai fait dans le domaine du DNSSEC. Je suis co-fondateur de ma société. Vous aurez peut-être vu les algorithmes que j'avais préparés et les chiffres de notre présence en Norvège.

J'habite dans le secteur délimité en vert, au milieu, et on a à peu près 50 mairies qui ont leur DNS enregistrés et qui sont les titulaires de leur propre nom de domaine.

On avance. Je suis responsable de 30 000 abonnés et des résolveurs de DNS de ce petit secteur. Nous allons tous les garantir avec cette offre de confiance du RFC 50-11. Ils ont tous des résolveurs à différents niveaux. On espère que ça va fonctionner.

Quand on nous a invités à cette conférence, on s'est dit qu'il allait falloir que l'on examine ces questions de [outbound] et de [bound] et faire confiance à ce que tout se passe bien.

Mais nous avons également mis en place plusieurs résolveurs de validation pour les entreprises. Je ne sais pas très bien combien l'ont fait, mais nous, on les utilise pour des questions de performance et de facilitation de service. Voilà donc notre

situation concernant le roulement de la clef KSK. J'espère que ça va fonctionner.

Je pense qu'on a une diapositive de plus. Oui. Vous avez peut-être entendu parler de différents incidents ayant eu lieu il y a 10 ans. C'était moi qui avais signé [inaudible] .se, vous pourrez le lire. Ce n'est pas une question de validation. Tout est clair dans tout ce que j'évoque ici dans ma diapo.

Je dirais qu'avant de créer les signatures de la racine, on a eu des problèmes de KSK, lorsque le .SE a roulé sa propre clef, mais une fois que la racine a lancé sa propre signature, on n'a plus eu de problèmes.

Parfois, on entend dire que les gens s'inquiètent de la taille double des clefs. Mais en Suède, on avait plus d'une centaine de clefs ne fonctionnant pas et on est parvenu à les résoudre correctement, même si elles étaient plus grandes. Donc je ne m'inquiète pas de la taille de cette nouvelle KSK et de la coexistence des deux.

Voilà, c'est tout.

DAN YORK : Il faut noter que Torbjörn a un t-shirt qui dit « DNSSEC, c'est fait ».

Y'a-t-il des questions pour lui ? Oui ? [Inaudible]

INTERVENANT NON-IDENTIFIÉ : Merci, Torbjörn. Chaque version, à partir de 2011, va, en fait, résoudre votre problème par rapport au roulement de la KSK.

Vu votre expérience, je pense que chaque année, il faudrait commencer à rajouter à cette chaîne créée en 2011 pour que ça fonctionne correctement. Ensuite, dans votre cas, puisque vous êtes un petit fournisseur et que vous fournissez les PME, vous auriez encore moins de problèmes en utilisant cette ancre 50-11, pour identifier les problèmes ou si vous avez des procédures en place vous permettant de télécharger la nouvelle ancre de confiance du site Web de l'ICANN.

[TORBJÖRN EKLÖV] : Je vérifierai avec certaines de mes résolveurs s'ils le font bien.

DAN YORK : Des questions pour Torbjörn ? Non ?

Super. On avance rapidement. Je suppose que la réponse, c'est qu'en fait, ce panel n'était pas nécessaire parce que c'est simple et accompli. Très bien, on s'attendait à cette réponse. On va passer au plus complexe et nous demanderons à Andre de parler des marchés plus complexes, du marché des FSI dans son cas.

[ANDRE] : Merci. On ne s'est jamais vraiment concentrés sur cette question, les gens n'y font pas tellement attention, mais je pense que le rôle des institutions impliquées dans les infrastructures Internet est justement de travailler dessus.

Lors du dernier panel auquel j'ai participé, on avait élaboré différents contrôles et freins pour les widgets. Malheureusement, on n'a pas pu trouvé de moyen pour démontre que les résolveurs sont correctement en conformité avec le RFC 50-11.

Si vous avez les moyens de le prouver, faites-le moi savoir car ce serait intéressant de le faire pour faire avancer la racine en ayant ce type de contrôles et de vérifications. C'est un problème pour nous actuellement.

C'est pourquoi nous essayons de communiquer autant que possible avec la communauté des FSI. On a un certain avantage parce qu'avant la signature de clef, il y a eu cette check zone qui a été installée comme zone de confiance et qui a, par la suite, été mise à niveau et est devenue la zone digne de confiance.

Donc, on a cette ancre de confiance maintenant que nous mettons à jour de temps à autre. Nous sommes constamment en contact, nous parlons directement avec les mainteneurs, nous

tenons des conférences où nous discutons ces questions et nous avons de très bons rapports avec les points d'échange Internet locaux, ce qui rend le groupe des opérateurs de réseau plus simple.

S'il y a une réunion des FSI, on les invertit des mises à jour, des nouveaux risques associés au DNS, on leur dit comment les aborder. La distribution se fait correctement grâce au serveur que nous avons installé, donc on ne devrait pas connaître de problèmes.

Parfois, nos FSI trouvent différentes solutions, donc on les analyse avec eux et on discute avec prudence pour vérifier que leurs solutions sont correctes. Je pense qu'ils y arriveront, on ne craint donc pas le jour J.

DAN YORK : Très bien. Je suppose qu'il n'y a pas aucune inquiétude, tout le monde est content et confiant pour la date du 11 octobre. Matt, pas la peine de parler, c'est bon, on a compris.

Warren, qui est ici à côté de moi, a peur, il appréhende un peu ce jour. Voyons ce qu'en pense [Erwin] ? Irez-vous aussi vite ?

[ERWIN LANSING] : Oui, bien sûr. Je vais répéter un peu ce que disait Andre. Du côté danois, on a du personnel technique qui connaît bien le système et il faut s'assurer que tout le monde sait bien ce qui va se passer et est en conformité avec le RFC 50-11 quelques jours avant le lancement de la nouvelle clef, puisque le roulement de la KSK en dépend.

Hier, le groupe des réseaux d'entreprises danois a lancé un appel et un communiqué pour s'assurer que tout le monde était au courant de ce roulement de la clef. D'autre part, il y a des projets de logiciels qui nous intéressent aussi et sur lesquels nous travaillons. Vous en avez peut-être entendu parler.

Donc, ça c'est pour le côté public, mais il faut également que, du côté des utilisateurs, tout le monde aura la capacité adéquate pour télécharger les informations et les paquets des opérateurs, et que, bien sûr, les systèmes d'exploitation qui ont commencé à inclure ces validations dans leur propre système d'exploitation utilisent les bonnes versions et les bons mécanismes, de sorte que les utilisateurs mettent à niveau leur DNS et que tout fonctionne correctement.

Malgré tout, il y a des domaines qui m'inquiètent, ce sont les boîtes noires. Les boîtes noires qui font cette validation de DNSSEC ne sont pas toujours quelque chose de connu parce que ça fonctionne tout seul, et puis un bon jour, ça s'arrête et ça ne

fonctionne plus. Ce sont des boîtes qui sont dans un sous-sol, personne ne sait qu'elles existent ni ce qu'elles font ou comment elles fonctionnent et on ne sait pas quoi faire. Il y a des gens qui ne savent même pas que le DNS existe ni ce qu'est le DNSSEC. Voici ce qui nous inquiète.

DAN YORK : Paul, vous voulez rebondir sur ce point ?

[PAUL EBERSMAN] : Oui, je pense qu'aux États-Unis, le principal problème était pour le .GOV. Lorsqu'ils ont mandaté les DNSSEC, ils ont ajouté beaucoup d'espace de stockage pour ces extensions de sécurité, sachant qu'il y a eu des réductions budgétaires, pas mal de gens ont dû commencer à s'inquiéter de cela, puisqu'ils n'avaient plus les mêmes espaces. Il faut continuer à travailler à la validation, ils se penchent là-dessus. [Roland] est très au fait de cela.

DAN YORK : D'autres commentaires ? D'accord, très bien.

Roland, je sais que vous allez partager certaines mesures.

[ROLAND LaPLANTE ?] : Non, ce sera plus tard. Pour l'instant, je vais vous raconter ce que je souhaite faire.

Diapo suivante, s'il vous plaît. Bien.

Les actions des opérateurs figurent toutes sur cette diapo. Vous voyez que nous allons mettre en œuvre les unbound 1.6.1 dans l'ancre unbound ou illimitée. On appelle ça le jour K, et non pas le jour J, car pour nous c'est le 11 juillet le jour clef, le jour où nous allons commencer et lancer le processus. Pour nous, c'est à partir de cette date qu'il faudra faire le suivi de ces fichiers.

Pour ma part, je vérifierai que les référentiels des zones de confiance sont correctement reçus par les résolveurs, que ce soit correctement traité. Je fais confiance à mon logiciel, c'est vrai, mais il faut quand même s'assurer que le système de fichier puisse écrire partout avec cet unbound, qu'unbound puisse être traité par tout le système.

Dans le même temps, nous informons les opérateurs de notre unité constitutive, de notre réseau d'éducation et de recherche des pays bas où on a beaucoup de gens impliqués. Certains font leur propre trafic, certains font passer leur trafic par nos systèmes et on les avertit tous de ce qu'ils doivent faire. Les utilisateurs, dans notre unité constitutive, sont très différents. On a des personnes qui font de la résolution à travers des iPads,

par exemple. Il serait intéressant de voir s'ils sont en mesure de traiter correctement la nouvelle KSK.

Je voudrais parler d'une autre idée que j'ai eue et dont j'ai discuté. C'est une idée qui porte sur unbound, et j'en ai discuté avec [Roy ?] du Pays de Galles de l'ICANN par exemple, pour mesurer le roulement de la clef de signature de clef.

J'essaie de trouver une bonne photo d'un [canari dans une mine de charbon] pour vous montrer ce qu'on faisait auparavant. Vous connaissez le système, n'est-ce pas ? Bon, certains ne connaissent pas.

C'est remarquable – à l'époque où on utilisait les mines pour extraire du charbon faute d'énergies renouvelables, les mineurs utilisaient des oiseaux qu'ils emmenaient, en cage, dans la mine. L'idée était que, comme les oiseaux sont si sensibles aux gaz, si l'oiseau commençait à se sentir mal ou s'il mourrait tout court, c'était un signe qu'il fallait qu'ils abandonnent la mine, parce qu'il y avait une fuite de gaz.

Notre idée était de faire quelque chose de similaire pour le roulement de la KSK. Mon idée est d'avoir un oiseau dans la mine virtuelle pour pouvoir faire un suivi de l'impact opérationnel au moment d'exécuter le roulement de la KSK, pour agir comme un signal d'avertissement comme quoi les

résolveurs de validation n'arrivent pas à valider à partir de la nouvelle clef.

En fait, j'ai deux objectifs parce que moi, en tant qu'académique, je voudrais pouvoir rédiger un document à ce sujet, donc je veux obtenir ces données et ces mesures de la validation pendant le roulement de la nouvelle KSK, pour pouvoir observer ce qui se passe pendant ce type d'evénements.

Ici, sur cette diapo, on voit que l'idée est d'aborder la question à partir de quatre points de vue, avec quatre mesures différentes. Utiliser d'abord [Luminati ?] qui vérifie les contenus des États-Unis à travers des services de déblocage. Vous connaissez ça, n'est-ce pas ? Levez la maint, vous le faites tous.

Il y a ici certaines entreprises qui offrent des services VPN gratuits, et si vous les utilisez à titre gratuit, vous leur donnez votre ordinateur comme un nœud de sortie de trafic. C'est bien parce que ça vous permet en même temps de faire des enregistrements et de mesurer le trafic qui passe par votre ordinateur. Vous pouvez le faire autrement, mais vous n'aurez accès qu'à des réseaux résidentiels.

Moi, je veux voir avec Luminati si on ne pourrait pas appliquer cette méthodologie pour mesurer la validation dans ces nœuds. Luminati est présent dans beaucoup de réseaux résidentiels

partout dans le monde, c'est ça qui est intéressant comme point d'itération.

Je travaillerai également avec APNIC qui fait constamment des mesures de DNSSEC pour essayer d'inclure ces mesures dans mon étude. APNIC travaille déjà sur ces données, on peut déjà commencer à les analyser.

Je travaillerai également avec RIPE ATLAS, et enfin je mesurerai le trafic au serveur de nom racine. Il y a des gens qui prévoient de le faire pour évaluer si les personnes font de nouvelles versions des clefs et si tout est corrigé, et quel est le trafic.

Mon idée est donc d'établir un point de référence des validations avant le jour K, pour mesurer le signal et le bruit qui en sort. Si on mesure ce bruit, il y aura des intermittences dans les signaux – parfois ils seront validés, parfois non, assurément.

Mais mon idée principale est de faire ses mesures au quotidien, et peut-être d'augmenter la fréquence, si possible ou si c'est souhaitable. J'imagine que plus on approchera du [11 octobre], plus on pourra augmenter cette fréquence, dans les fournisseurs résidentiels au moins, pour augmenter la fréquence.

J'espère que l'on pourra prendre des mesures là-dessus. Si l'oiseau commence à chanter ou s'il meurt, on se rendra compte si des opérateurs ont des problèmes avec les résolveurs de

validation ou non, et on pourra les contacter pour les informer du problème. On leur dira « vous avez un gros problème ici, il va falloir vous en occuper».

On travaillera donc avec la communauté des opérateurs et, si on peut le faire en tant que communauté, on pourra s'assurer que ce roulement de la KSK ne sera pas le chaos mais le succès que l'on espère.

Diapo suivante. Mon plan est de commencer à travailler la quatrième semaine du mois d'avril pour commencer ce qui se fait, comment recueillir les informations, quelles informations recueillir. Si vous avez des idées, bien sûr, je vous en serai reconnaissant. Je travaillerai sur rootcanary.org. C'est un site tout simple. L'idée est d'avoir une conception plus intéressante.

INTERVENANT NON IDENTIFIÉ : Est-ce un site signé DNSSEC ?

[ROLAND LaPLANTE] : Non. C'est fait exprès, d'ailleurs.

Je crois que c'était ma dernière diapo, il me semble que j'ai fini. C'est bien le cas ? D'accord.

Est-ce que vous avez des questions ou des suggestions ? Si c'est le cas, je suis là pour vous répondre. Vous pouvez aussi m'envoyer des mails.

DAN YORK : Je pense qu'il y aura des questions, mais j'en une moi aussi.

Le serveur Luminati est un serveur VPN gratuit que vous utilisez pour convertir vos ordinateurs en nœuds ?

[ROLAND LaPLANTE]: Oui, tout à fait. Vous savez que, d'habitude, on lit les conditions de service, mais en fait personne ne les lit et dit simplement être d'accord. Dans leurs conditions de service, vous leur donnez le droit d'utiliser votre ordinateur comme nœud.

DAN YORK : C'est bien de le savoir. Je n'utilise pas ce service actuellement mais je garderai ces informations en tête.

Donc, on a Warren.

WARREN : Revenez deux diapos plus tôt, s'il vous plaît. Par rapport à ces mesures DNSSEC d'APNIC, je voudrais vous dire que George est en train de travailler là-dessus et prévoie de faire ces mesures à

mesure que la KSK sera roulée, et qu'il fournira ces informations à l'ICANN. Il travaille avec une autre personne et ils vont essayer de faire ça rapidement. Que je sache, les serveurs racine vont eux-mêmes faire ce type de mesures au cours de cette période spécifique et mettront ces données à notre disposition. Pourrait-on revenir encore en arrière ?

[ROLAND LaPLANTE]: Oui, je n'ai pas expliqué pourquoi on voulait le faire de différents points de vue. C'est parce que si on ne considère que les données d'APNIC, on a une certaine visibilité, mais le problème avec les mesures DNSSEC provenant seulement d'APNIC est qu'on ne peut pas reproduire les mesures au même emplacement en toute fiabilité, on dépend du réseau. Donc, ça donne de bonnes informations mais ça ne peut pas être reproduit, alors que Luminati vous permet de choisir le nœud de sortie pour avoir une reproductibilité bien meilleure, ce qui fournit davantage de données que ce vous donne APNIC. On essaie donc d'en profiter pour améliorer cette initiative autant que possible.

WARREN : Dans cette diapo précédente, ce que je pense, c'est que si la validation s'arrête tout court, toute la résolution de DNS va échouer, en fait, d'après ce que vous dites. Donc, tous les

opérateurs se rendront compte qu'ils ont problème, ce n'est pas la peine de les informer.

Est-ce qu'on peut poser des questions générales maintenant ? C'est ça ma question générale pour les gens comme ComCast. J'imagine que vous avez une population qui vous fait suivre des requêtes et fait la validation.

Est-ce que vous savez de combien d'acteurs il s'agit ? Parce que si vous agissez et qu'ils font leur propre validation, ils vous appelleront si ça ne fonctionne pas, pour différentes raisons, bien sûr, parce que c'est vous le fournisseur. Les gens veulent faire fonctionner leur propre serveur de nom et n'ont pas de système unbound ou parce que Julie, Dan, Steve ont beaucoup travaillé dans les atelier DNSSEC pour les débutants, les gens penseront aux clefs et vous contacteront pour vous demander de les aider.

Donc, pour valider les résolveurs, par exemple, est-ce que vous savez quel est le pourcentage d'utilisateurs qui font leur propre validation ?

D'autre part, avez-vous discuté de cela avec les techniciens pour qu'ils soient prêts à fournir ce support technique dès qu'ils seront appelés pour ce type de problèmes, pour qu'ils puissent expliquer au public comment exécuter le DNSSEC ?

PAUL EBERSMAN : Non, on ne sait pas très bien comment vérifier que les gens se trouvent dans la chaîne de résolveurs. Malheureusement, tout se fait par défaut de nos jours, et la première personne à contacter, c'est toujours nous et c'est un peu complexe de ne pas savoir ce qui est paramétré. On a une idée assez claire de ce que font les autres personnes qui exploitent des résolveurs au sein de notre entreprise. On a des balayages et des cartes de repérage pour essayer de faire le suivi de toutes ces activités. Un groupe a commencé à utiliser [n-map] récemment. C'est le même système, ils ont la même automatisation, donc on est en mesure de les contacter pour leur demander de résoudre certains problèmes. Or le groupe des FSI se plaint du CPE et d'autres mises à jour. Nous avons obtenu des systèmes qui soutiennent le DNSSEC, on a ajouté le codage nécessaire à ces logiciels. Si vous voulez en reparler par la suite, Erwin, vous pouvez venir me voir, mais nous ne pouvons pas configurer le fichier qui déclenche ces activités.

La plupart des FSI sont prêts pour le CPE et d'après ce que nous savons, la plupart de ceux qui sont prêts sont ceux pour lesquels nous contrôlons le système et, dans leur cas, c'est nous qui sommes les propriétaires des mises à jour. Il nous faudra donc communiquer avec ceux qui ont XP3 ou un des dispositifs de CPE. Pour l'instant, on n'a pas communiqué avec ceux qui

travaillent [en première ligne]. Ce sera une véritable difficulté. En général, le DNSSEC a été assez problématique et malheureusement, il arrive que les gens pensent que c'est un problème de DNSSEC, ce qui me retombe dessus. Voilà où nous en sommes, en fait. Voulez-vous rebondir ?

INTERVENANT NON IDENTIFIÉ : Oui, pour les versions de logiciel, les firmwares, il y a différents avertissements qui vont vous dire que vous pouvez télécharger une nouvelle version qui va résoudre tel ou tel problème.

PAUL EBERSMAN : On n'a pas de visibilité, on ne peut pas faire cela, et comme pour d'autres CPEs, on choisit notre propre version. Maintenant, il est possible de choisir qui sera le vendeur de logiciel donc ce sera un peu compliqué de travailler avec les vendeurs, de sorte qu'ils fassent les mises à jour des CPEs.

DAN YORK : Roland, voulez-vous répondre ?

[ROLAND LaPLANTE] : Oui, j'ai deux remarques. Warren disait que les grands opérateurs ont un mode échec qui ne fera probablement aucun

type de résolution à partir du moment où ils auront des problèmes de validation. On a vu des problèmes de validation avec certains TLDs, en cas d'échec de l'algorithme ou en cas de défaillance, et ce qu'ils faisaient consistait à effacer tout le TLD. Donc, s'il y avait des problèmes dans la racine, toute la racine disparaitrait dans cette logique. On espère que ce ne sera pas le cas.

Mais il y a deux autres aspects qui pourraient être problématiques. Dans le roulement de la KSK dans la racine, à un moment donné, la clef sera très longue. Cela pourrait représenter des défaillances intéressantes qui n'impliquent pas que la résolution ne se fasse pas du tout à aucun moment.

D'autre part, on a la distribution et les limites de ce qu'on a et de ce qu'on a eu, et lorsque nous aurons la nouvelle version déployée, il faudra vérifier tout cela fonctionne correctement. J'ai commencé à essayer des mesures du côté des serveurs faisant autorité, pour la validation DNSSEC et il y a énormément de résolveurs qui ne desservent qu'une petite population de clients, mais la quantité de résolveurs augmente très rapidement, et ce sont ces serveurs qu'il faudrait que l'on contrôle.

ROY : Je pense que c'est une excellente idée, cette idée du canari. J'ai vu la proposition pour la première fois il y a quelques semaines et dans notre équipe, à l'ICANN, nous avons trouvé cela fantastique, nous avons été très enthousiastes. Nous avons nos propres données, les données de la racine L que nous collectons et ce que nous voudrions, c'est savoir ce que va donner cette étude.

Est-ce que c'est pour la période complète du roulement de la clef KSK ou bien pour quelques jours ?

INTERVENANT NON IDENTIFIÉ : Ce n'est pas exactement une question pour moi, mais c'est plutôt une question qui a été posée à plusieurs reprises. Que se passe-t-il si le roulement n'aboutit pas ? Et la question est de savoir ce qui se passera avec les opérateurs. Il faudrait avoir des informations de dépannage - comment résoudre un problème que ce soit manuellement ou non, donc notifier les opérateurs qu'ils doivent mettre certaines actions en place. Ces informations devraient exister quelque part pour que les gens puissent les récupérer. Si les choses ne fonctionnent pas, vous pouvez essayer les actions suivantes, par exemple. Ou bien avoir un site Web avec des instructions spécifiques.

Je ne veux pas créer une surcharge de travail, c'est une question, pour voir si cela pourrait être mis en place.

INTERVENANT NON IDENTIFIÉ : Je pense que c'est une bonne idée. Ce serait intéressant que l'on puisse appliquer des mesures de correction si la résolution ne peut pas se faire. Mais, bien entendu, il faudrait faire cela dans un domaine qui ne soit pas signé. Je pense que c'est une bonne idée de le faire et ce serait un effort conjoint pour que l'on puisse produire des paquets ouverts avec différentes étapes pour appliquer des mesures de correction.

DAN YORK : Matt, est-ce que vous êtes là ? Je ne veux pas parler en son nom, mais je sais que les gens de l'ICANN réfléchissaient déjà à créer une base de dépannage disponible et nous pourrions donc envisager le fait que cette base soit disponible dans un domaine non-signé, bien sûr.

PAUL EBERSMAN : Allô ? Je me demandais, est-ce qu'il y a une adresse IP que tout le monde connaîtrait, ou qui pourrait fonctionner alors que toutes les autres ne fonctionnent pas ? Ce serait intéressant d'avoir ses informations là-bas.

INTERVENANT NON IDENTIFIÉ : Pour ceux qui écoutent à distance, c'est Warren de Google.

ED LEWIS : Bonjour. On est en train de penser à résoudre un problème, mais je voulais dire que s'il y a une ancre de confiance dans votre résolveur, le problème n'est pas de savoir où on met cela, mais plutôt où mettre le signal d'alerte.

DAN YORK : Signal d'alerte d'internet. Ce n'est pas bien.

[ED LEWIS ?] : Il y a un risque que vous ne puissiez plus résoudre vos résolveurs.

DAN YORK : Très bien, on a bien compris.

[ROLAND LaPLANTE]: Est-ce que je peux ajouter un élément ? Si on fait des recherches de DNS inverse, on ne pourrait même pas accéder à une machine.

DAN YORK : Très bien.

J'ai Oliver et [inaudible] au micro.

OLIVER : Je pense que les gens vont pouvoir ouvrir deux ou trois résolveurs et donc, si quelque chose ne va pas, cela affectera une petite population et je pense que les clients pourront accéder à une autre boîte.

Mais je comprends bien qu'on essaie de voir les choses globalement, donc je trouve cette idée intéressante, aussi il faudrait inviter ceux qui souhaiteraient participer à cette initiative pour qu'on puisse avoir des informations partagées.

Ensuite, nous avons un canal de communication quand les choses ne marchent pas, à savoir Twitter, donc pourquoi ne pas traiter un hashtag #roulementKSKavertissement pour pouvoir faire un suivi de comment les choses se passent.

DAN YORK : Il faudrait demander à tous les trolls et les spammeurs sur Twitter.

Aurons-nous le nom officiel au 11 juillet ?

[Inaudible].

INTERVENANT NON IDENTIFIÉ : Ma question est pour Roland. Le canari paraît très important pour les opérateurs, donc j'essaie de savoir si c'est possible ? Parce que si les opérateurs voient que quelque chose se passe, ils vont se diriger vers les opérateurs racine. Cela m'inquiète. Les informations sont importantes, mais après, comment allons-nous distribuer ces informations aux opérateurs ? Dan, [Olivier] pourrait-il nous aider ?

DAN YORK : Oui, il y a plusieurs personnes qui pourraient avoir accès à ce type d'actions et qui pourraient participer.

Warren ?

WARREN : Oui. Dans plusieurs documents SSAC, comme dans le SSAC63 - il y a beaucoup de gens qui ne participent pas et nous avons eu beaucoup de succès avec le DNS. Si vous voulez mettre en place le DNSSEC, c'est quelque chose de génial, on a donc beaucoup insisté pour sa mise en place.

Mais là, ce qui me fait peur, c'est le nombre de gens qui ont validé le DNSSEC parce qu'on leur a dit que c'était ce qu'il fallait faire. Je me demande maintenant s'il y a des aspects que l'on

n'arrive pas à gérer, et alors ils pourraient carrément ne plus valider le DNSSEC. Alors, je ne sais pas, mais je voulais vous demander ce que le roulement de la KSK implique pour vous.

Je pense que, malheureusement, quand les choses ne se passent pas bien, les gens vont directement ne plus valider le DNSSEC, parce que c'est le moyen le plus facile d'éviter le mal.

DAN YORK : Je pense que vous avez raison.

INTERVENANT NON IDENTIFIÉ : D'après mon expérience avec les failles de DNSSEC, dans la plupart des cas, ce n'est pas un problème de roulement de clef, mais parfois, il s'agit de problèmes au niveau de la signature et c'est un problème que l'on peut – oui, c'est vrai que lorsqu'il y a un problème, ils arrêtent le DNSSEC.

[PETER ?] : Quand les gens modifient la configuration du résolveur pour valider une clef ou en installer une nouvelle, ils peuvent non seulement détruire certains éléments mais aussi directement interrompre le fonctionnement et déconnecter le TLD.

DAN YORK : Combien de gens dans la salle ont changé la configuration d'un résolveur DNSSEC dans les six derniers mois ? Oui, c'est vraiment ce que je voulais savoir, bien.

Maintenant, si nous étions une population en dehors de cette salle et en dehors de l'ICANN, combien de gens ont changé régulièrement la configuration du DNSSEC au cours de la dernière année, selon vous ? Voilà, c'est ça.

Je pense qu'on est en train de compliquer les choses. Je vais reformuler ma question et peut-être aurais-je plus de réponses, parce que tout le monde a tendance à très vite lever la main.

INTERVENANT NON IDENTIFIÉ : Alors, mettre à jour le logiciel pour que les gens ne s'en rendent pas compte, pour calmer un peu les choses, mais au niveau des utilisateurs finaux, cela pourrait être utile.

DAN YORK : La question est de savoir quand, par exemple, les gens achètent le boîtier et font ce que disent les instructions, c'est tout du moins ce que l'on fait aux États-Unis et c'est très bien, sauf qu'en général ils ne s'en servent plus et les configurations vieillissent aussi. Je me demande, maintenant, s'il y a, au niveau des logiciels, par exemple Microsoft – la raison pour laquelle je pose

la question, c'est que j'ai eu un échange avec quelqu'un qui déployait le DNSSEC.

Ils utilisaient l'un de nos serveurs d'autorité en tant que serveur secondaire, et j'ai été surpris parce que je n'avais jamais vu de comportement dans le serveur Windows 2012. Ce qui m'inquiète, c'est que c'est le cas pour la validation aussi, donc la bonne nouvelle, c'est que si vous êtes un utilisateur Windows légitime, Microsoft sait quelles sont les rustines que vous avez mises en place ou non.

Je me demande si c'est le cas pour d'autres grandes plateformes comme Red Hat, s'il y a une certaine visibilité permettant de savoir combien de gens ont téléchargé les paquets, et savoir s'ils ont les outils pour gérer ces situations.

DAN YORK : Je pense que la personne au micro pourrait nous apporter une réponse.

[PAUL EBERSMAN] : Nous avons certaines statitsiques, mais il y a des gens derrière des serveurs proxy donc on n'a pas de mesures exactes. Dans notre cas, la situation est plus simple parce que nous passons directement à de nouvelles versions de logiciels.

La politique de Red Hat, c'est qu'il faut avoir des logiciels stables et qui ne changent pas. Si vous trouvez que cela doit être amélioré, il faut créer un nouveau logiciel ou en créer une nouvelle version. Parce qu'à moins que les clients nous demandent de sortir une nouvelle version, nous gardons la même version stable.

DAN YORK : Très bien. Est-ce qu'il y a d'autres questions ?

Allez-y, les gens assis au fond de la salle. Est-ce qu'il y a des gens de FSI souhaitant nous poser une question ou nous raconter ce que vous avez fait. Très bien, [inaudible] ?

INTERVENANT NON IDENTIFIÉ : Un commentaire pour les gens de l'ICANN. Je sais qu'il y a un souci par rapport à la taille des clefs. Je pense que ceux font validation DNSSEC se rendent compte que les paquets deviennent de plus en plus gros et que cela devient problématique.

Alors, le problème de roulement de clef DNSSEC, ce n'est pas le roulement en lui-même, mais plutôt la taille du paquet toujours plus importante.

DAN YORK : Vous avez l'air de vouloir dire quelque chose.

INTERVENANT NON IDENTIFIÉ : Oui, Si vous achetez votre dispositif CPE, vous faites confiance à votre fournisseur.

Warren a parlé des signaux d'alerte et je pense que c'est un aspect important.

[BERT ?]: Bonjour. D'un côté, nous ne pouvons pas voir les versions de logiciel que possèdent les utilisateurs, ce qui permet de faire des déploiements plus sélectifs. C'est justement ce que nous faisons, n'ayant pas encore déployé le RFC 50-11, et il faut qu'on fasse bien les choses.

Ensuite, je voulais que, comme Paul, on a des proxys pour la communauté des opérateurs et la situation est assez compliquée. Je me fais l'écho de ceux qui pensent que les gens vont tout simplement désactiver le DNSSEC en cas de problèmes.

Alors, ma suggestion est de dire à tout le monde combien il est important de bien faire les choses et de faire la mise à jour avant. Mais en plus, il faudrait avoir déjà préparé des documents pour les gens qui ne nous écouteront pas, et dire « voilà des

instructions qui pourraient vous aider, si vous ne faites pas ça, ça pourrait mal se passer ». Les grands fournisseurs de services Internet en Europe ont 0,4% des gens qui travaillent sur le DNSSEC.

DAN YORK : Très bien. Merci beaucoup pour votre travail au fil des années, au niveau du DNSSEC et des statistiques. Donc, merci beaucoup pour votre travail dans domaine.

Est-ce que quelqu'un veut dire quelque chose par rapport à ce que [Bert] vient de dire ?

INTERVENANT NON IDENTIFIÉ : Je serais curieux de savoir quelles sont les parties du RFC 50-11 que vous n'avez pas mises en œuvre.

BERT : Nous sommes sept et ces sept personnes ont des opinions très intéressantes, donc je les écoute, puisque moi-même je ne sais pas.

DAN YORK : J'aimerais bien lire les tweets.

MATT LARSON : Matt Larson, ICANN. Je sais que l'on doit produire un document comme celui qui vient d'être évoqué. Nous avons des présentations avec lesquelles nous allons travailler d'ici à ce que la clef soit roulée et ces informations figureront sur une page Web à laquelle vous pourrez accéder.

DAN YORK : Oui, Matt, je réfléchis à une façon de collaborer tous ensemble de façon très simple et directe, un peu comme le canari dont on a parlé. À savoir, si le DNSSEC ne fonctionne plus, voici ce que vous devez faire.

MATT LARSON : Je ne sais pas vraiment quelle forme cela va prendre, mais oui.

DAN YORK : L'idée est de faire quelque chose d'assez clair. Nous pourrions donc réfléchir collectivement à comment faire ça de manière simple pour les utilisateurs.

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

Alors, on va parler du rapport 2017 sur le roulement KSK. Vous travaillez là-dessus, donc nous pourrions en parler et voir si, à la prochaine réunion, on pourrait en discuter.

[ROLAND LaPLANTE]: Oui, bien sûr.

DAN YORK : Très bien. Avons-nous d'autres choses pour ce panel sur le FSI ?

Dans ce cas-là, nous allons applaudir nos panelistes.

Maintenant, nous allons passer à une démonstration. Nous allons faire preuve de courage et regarder cette démonstration.

Pendant qu'on prépare, nous n'avons pas encore dit que [Torbjörn], ici est derrière un certain nombre de statistiques – vous en avez parlé un peu – pour le DNSSEC, l'IPv6. J'ai toujours voulu le rencontrer, car c'est lui qui a écrit beaucoup d'informations en relation avec l'IPv6. Vous pouvez aller sur CircleID.com, vous pourrez y lire ce qu'il a écrit par rapport à l'IPv6 et son histoire, IPv6 dont il est le bouc-émissaire. Et on sait qu'il y a toujours des remarques sur l'IPv6 et qu'il y a toujours des informations à ce sujet.

On discute un peu pendant que la démonstration se prépare.

Cette discussion sur les bouc-émissaires et sur les boucs nous conduit vers des statistiques intéressantes. C'était au Texas. Le site ne fonctionne plus actuellement. Il y avait une nouvelle version, mais nous n'avons pas eu le temps de la réparer. Le but

était de fournir des informations sur les différents comptes au Texas qui avaient adopté IPv6.

Nous arrivons à notre présentation où nous voyons des lignes de commande à l'écran.

Nous allons voir si Paul peut nous parler de l'IPSEC et voir comment il le rend intéressant pour une présentation.

PAUL EBERSMAN : Je fais partie du projet [librephone ?], à savoir le signe « libre » que vous voyez à l'écran créé par John Gilmmer de l'EFF. L'idée de ce projet est de chiffrer toutes les informations qui passent par le DNSSEC. Nous n'en sommes pas encore là, mais nous y travaillons. La raison pour laquelle cette équipe travaille sur le DNSSEC, c'est qu'ils voulaient mettre des clefs publiques sur le DNSSEC pour pouvoir les décharger de manière sécurisée et les utiliser dans les machines en toute sécurité. Nous envisageons donc d'utiliser une base de données distribuée sécurisée pour récupérer les clefs.

Quelques diapos pour expliquer les choses. Quand on pense au VPN, on a un VPN de site à site où on connecte deux nuages ou deux sous-réseaux et où la communication entre ces nuages n'est pas chiffrée, ils sont visibles. Et les serveurs IPv6 ont des données chiffrées. Ce n'est pas une situation idéale mais c'est

courant. Nous voyons un encouragement assez important à chiffrer toutes ces composantes individuelles. Bien sûr, on aimerait utiliser IPSEC pour cela.

Voici un tunnel VPN que vous connaissez parce que vous pouvez l'avez chez vous, dans vos bureaux. Vous avez les routeurs qui se connectent à un serveur, serveur qui est connecté au nuage. C'est un modèle utilisé par Netflix pour les gens qui ne sont pas aux États-Unis. Les gens se connectent sur leur VPN dans leurs ordinateurs et peuvent accéder à Netflix aux États-Unis.

Maintenant, qu'est-ce que l'IPSEC opportuniste ? Nous avions besoin de certaines fonctionnalités que nous n'avions pas il y a 15 ans. D'un côté IP version 2, c'est un protocole utilisé dans le tunnel VPN. Nous n'avions pas de manière symétrique et si on va dans un tunnel dont la connexion est chiffrée, il faut pouvoir d'authentifier le serveur, mais le serveur ne sait pas qui vous êtes puisque vous êtes anonyme. Donc avec IP version 2, nous y sommes parvenus. C'est important parce qu'avec IPSEC, il faut avoir la clef vous-même pour que votre ordinateur puisse être reconnu par le serveur. Avec IP version 2, ce problème est résolu.

On avait besoin du DNSSEC sur l'hôte local pour pouvoir mettre cela en place, et les résolveurs sont utilisés partout, ce qui pose un problème, car quand ils ont le DNSSEC maintenant, il n'y a plus d'insécurité entre les différentes parties. Cela nous permet

de faire des déclencheurs basés sur le DNSSEC. Nous connaissons le nom de celui qui envoie la requête, nous pouvons faire fonctionner l'application à travers le tunnel.

Nous devrions résoudre le problème de NAT. Si nous sommes derrière NAT, on voit une adresse IP et il nous fallait un moyen d'avoir plusieurs personnes connectées au même serveur sans provoquer de conflits.

Nous avons eu une idée. Nous avons créé une version préliminaire et le code LINUX nous a permis de l'installer. Tout cela est invisible avec IPSEC. Nous n'avons pas ajouté de règle qui pourrait produire des risques.

Voilà comment le paquet fonctionne. Nous avons une application – Firefox – et il faut se connecter. On va avoir le serveur DNS local qui n'est pas [inaudible]. Ce serveur local va trouver l'enregistrement DNS, va faire la validation DNSSEC, mais en parallèle, il va envoyer une requête à l'enregistrement IPSEC. Une fois qu'il aura reçu une réponse à ces deux requêtes, il continuera vers la deuxième étape du processus. S'il y a une clef IPSEC, il créera d'abord un tunnel IPSEC avec ces informations et c'est ensuite que le serveur DNS renverra l'enregistrement DN et des informations chiffrées seront donc captées dans ce tunnel.

C'est pour cela que l'utilisateur n'est pas au courant, c'est une utilisation opportuniste du DNSSEC. Si nous ne pouvons pas le faire de manière authentifiée, nous pouvons le faire de manière non-authentifiée. Ça ne remplace pas la barre d'adresse.

Ceci dit, j'ai fait un petit schéma pour mieux expliquer cela pendant ma présentation. Malheureusement, mon écran est un peu petit, donc je ne sais pas si on peut bien voir.

Tout d'abord, voici une machine. Nous allons voir ce qui se passe si je vais sur le premier serveur et que je ping. Donc, vous voyez, c'est pour avoir une ligne de base. Je fais un ping. C'est intéressant, non ? Ça a été rapide. Très bien. Vous voyez le ping. Vous voyez le texte en plain qui n'est pas chiffré. Maintenant, NAT ne dure pas longtemps ici. On va s'assurer de repartir à zéro et de voir s'il y a des tunnels. On nous dit que non.

Ça n'a pas été intégré au serveur DNS pour l'instant. Nous y travaillons, et nous avons besoin d'aide pour le faire. Actuellement, il s'agit d'un module indépendant dont le concept intégrerait le serveur DNS.

Ça fonctionne mieux si on lance ISPEC. On va le démarrer et recommencer. Voilà. On va revenir un peu en arrière pour que vous vous voyiez, ça va tellement vite. Vous voyez ici que vous avez l'enregistrement A, c'est comme un code python unbound.

On a ici l'enregistrement est protégé par le DNSSEC, on a l'enregistrement de clef IPSEC. On a téléchargé les donné.

Pour ceux qui ont déjà mis en œuvre le DNSSEC et ont déjà mis en œuvre les enregistrements de la clef IPSEC, je m'excuse si vous avez eu des problèmes. J'étais debout à une heure du matin, hier, pour finir cela, donc je suis au courant de vos souffrances, faites-moi confiance. Si on déchiffre cela correctement, on arrive à ce bloc de code qui est la clef RSA. Donc, on la télécharge et une interface renvoie cette clef vers le serveur IPSEC. Voyons si on peut avoir tout ça sur un même écran. Voilà. C'est l'équivalent de cette connexion.

Vous voyez qu'ici, à gauche, on vous dit que du côté du client, on utilise une authentification nulle, c'est-à-dire que l'authentification ne se fait pas du côté du client.

À droite, nous voyons la connexion, puis nous avons les termes IPSEC internes qui sont intéressants pour le monde du DNS. Puis, ça lance la connexion IPSEC. Vous voyez les échanges, les négociations, ça se met d'accord sur les clefs, ça lance le tunnel et ce dernier est finalement établi.

Pas de bytes ici, on va refaire le ping.

On voit que tout est correctement chiffré. On a plein de tunnels DNS qui sont établis à partir des données publiques du DNS.

Notre idée est de pouvoir accélérer cela et que ça se fasse par défaut pour avoir un chiffrement par défaut et que tout fonctionne correctement.

Y-a-t-il des questions ?

DAN YORK : Sérieusement ? C'est tout ? Il n'y a plus de questions, pas de doutes ?

[TORBJÖRN EKLÖV ?]: Vous n'avez parlé que des enregistrements A, qu'en est-il du code A ?

PAUL : En fait, le module comprend les deux, le code A aussi. Si vous avez 600 enregistrements A qui vous sont retournés, vous avez le choix d'établir 6 tunnels différents. Si vous êtes empêché de le faire et n'avez qu'un de ces enregistrements pour le tunnel, il va falloir décider si vous souhaitez mentir à l'application et ne lui rendre qu'un enregistrement. Que faire ? Ce sont les questions et les énigmes auxquelles nous devons répondre.

DAN YORK : Cette question était en fait de Torbjörn, c'est lui qui a suggéré cela.

On a d'autres personnes au micro.

INTERVENANT NON IDENTIFIÉ : S'il faut que j'intercepte un pare-feu et que c'est le pare-feu que je contrôle, comment gérer tous ces logiciels de nouvelle génération qui passent par dessus ce point-là et ne donnent pas le feu vert pour avancer ?

PAUL : Par rapport à la partie opportuniste, on ne donne pas les retours, le feedback aux utilisateurs, mais on veut se situer au niveau du dessous. On veut profiter du chiffrement sur Internet sans donner à l'utilisateur un site Web authentifié spécifique qui leur donne ce feu vert.

Si vous n'êtes pas d'accord et que vous voulez voir des textes de programmation sans arrêt, c'est possible. Donc, vous pouvez ajouter cela à l'application. Des gens l'ont fait avec l'adoption des [inaudible], et vous pouvez obtenir les feedback des clients. Mais, en définitive, ça finit toujours par des questions nous demandant comment nous comptons communiquer avec le client si ça ne fonctionne pas. On a donc décidé de ne pas lancer cette fonctionnalité pour l'instant.

Je pense qu'il va d'abord falloir qu'on lance ce code par défaut sur Internet, puis si vous voulez avoir des fonctions authentifiées

comme des paiements bancaires en ligne, il faudra vous assurer qu'à partir de l'application, tout fonctionne indépendamment de l'application que vous utilisez pour faire la validation.

PHIL : Je pense qu'il n'y a pas beaucoup de questions parce qu'en fait, tout le monde se demande pourquoi ça ne fait pas 25 ans que ça existe. C'est pas vrai.

Mais maintenant qu'on a la capacité de développer ce type d'application, c'est surprenant et c'est super.

Mais ne pourrait-on pas utiliser le DNS pour spécifier des politiques ? Vous l'a-t-on dit ?

PAUL : Non. L'un des échecs du projet précédent était qu'il permettait d'utiliser les clefs publiques du DNSSEC, puis une fois le DNSSEC lancé, ça ne fonctionnait pas vraiment. On pourrait donc dire que tout le trafic de [inaudible] 24 est passé au DNSSEC. Mais ça dépendra de cette possibilité d'avoir des données sécurisées et signées avec le DNSSEC. Que je sache, cet arbre inversé n'a jamais été disponible pour les utilisateurs et ça se fait de moins en moins, d'ailleurs. La moitié du temps, on n'arrive même temps à envoyer des mails à Google parce que ça ne fonctionne pas, mon IPv6 inverse ne fonctionne pas. Donc au moment où j'ai

eu cette idée de faire cette capture au niveau de l'IPSEC, j'ai vu que le problème est qu'on n'a pas cette possibilité d'inverser l'IPv6. Il nous manque une adresse de renvoi, donc on ne peut pas voir qui publierait des clefs en notre nom.

Donc, une fois que RPKI et d'autres initiatives seront lancées, les utilisateurs finaux auront d'autres possibilités pour assumer toutes ces tâches, pour accomplir toutes ces fonctions, mais pour l'instant, ce n'est pas possible. On a des problèmes et on ne peut pas faire face à tout le monde tout seul, vous savez qu'on me serait tombé dessus.

INTERVENANT NON IDENTIFIÉ : Oui, ce serait intéressant de voir comment vous lancerez votre session à travers le RPKI lorsque vous aurez ces modules.

PAUL : Oui, on a aussi des modules de backup. On permet ce trafic si ça ne fonctionne pas comme je viens de le montrer, mais on a aussi des groupes que l'on peut marquer et qui peuvent utilisé pour faire l'authentification, soit par certification, soit par des enregistrements DNSSEC qui s'authentifient entre eux. Malgré tout, il faut s'assurer qu'ils sont toujours chiffrés pour ne pas avoir de problèmes d'échec. Pour le 10 par 8, par exemple, c'est le seul pour lequel on a des chiffrements. On pourra faire des

exceptions. Certains clients ont dit que, pour des questions juridiques, ils ont dû arrêter leur trafic. Ça arrive.

Au moment de commencer à mettre en œuvre ce programme dans les réseaux internes, la moitié des pare-feu ne fonctionne plus, parce qu'on ne voit plus rien.

L'une des premières questions de l'un de nos premiers clients était de savoir si l'on pouvait montrer le numéro de port au moment de faire le chiffrement avec l'IPSEC pour savoir, au moins, quel était le port et permettre que le trafic passe à travers ce port.

On s'est dit que si on le faisait, les attaquants sauraient également quel est le port que vous utilisez et donc, ça n'a aucun sens d'avoir des pare-feu. Donc, l'idée est de distribuer la sécurité par d'autres mécanismes, ce qui sera plus simple.

INTERVENANT NON IDENTIFIÉ : Et Red Hat a vendu ? Non, ce n'est pas vrai.

PAUL: On passe pas Fedora d'abord. J'ai soumis ce paquet à RL 7.4 hier soir, à une heure du matin aussi, et cela contient déjà la capacité de chiffrement opportuniste pour ces paquets. Donc vous pouvez l'exécuter dans votre nuage interne si vous avez

certificats de CA et des certificats d'hébergement, vous pouvez déjà le lancer. Si vous êtes hôte de votre réseau, vous pourrez communiquer avec les autres hôtes de votre nuage.

DAN YORK : J'imagine que Paul dirait que si vous voulez que ce soit un logiciel qui vous appartienne et non pas Red Hat, il faudrait vous en occuper.

PAUL : Non, ce n'est pas la peine. C'est un de nos gros clients.

DAN YORK : Mais j'essaie de vous aider. Vous nous dîtes toujours de vous envoyer les rapports de défaillance.

PAUL : Oui, mais non, c'est pour les autres logiciels. Ici, ça ne nous intéresse pas.

DAN YORK : Carl ? D'autres questions ? Des remarques ? Non ? Pas d'autres questions pour Paul ?

Très bien, on remercie donc Paul de nous avoir fait cette démonstration en direct.

Comme je viens de le tweeter, on est probablement la seule salle de cette conférence à avoir des lignes de commande en cet instant, personne ne doit les avoir eues, j'imagine. Ça fait du bien de voir ces lignes de programmation.

Nous allons maintenant passer aux lignes graphiques. On passe des programmes aux graphiques. On a Roland avec nous qui va nous parler de l'ECDSA et de ce qu'il a trouvé dans ses travaux.

Roland, vous avez la parole.

[ROLAND VAN RIJSWIJK]: Merci, Dan. Il manque une diapo. Voilà.

L'idée est de nous concentrer sur l'adoption de l'ECDSA dans le DNSSEC. Ça vous donne un aperçu de trois gTLDs, un TLD spécial, très spécial d'ailleurs et sept ccTLDs. Ce travail a été fait en tant que chercheur et en tant qu'employé, j'ai donc ajouté les deux parties de ma recherche ici.

Vous savez probablement tous que l'ECDSA a été standardisé pour le DNNSEC en 2012 mais personne ne s'en servi jusqu'à ce qu'Oliver ait assisté à une réunion de l'ICANN et nous ait dit que le DNSSEC devait se faire en utilisant l'ECDSA, à partir du RFC 66-05.

Jusqu'à fin 2015, on ne voyait pas l'intérêt de l'utiliser. On avait moins de 50 domaines dans notre ensemble de données. En 2015, Cloudflare a annoncé le DNSSEC universel – je ne sais pas si vous connaissez. Cela veut dire que le DNSSEC est signé immédiatement à travers l'ECDSA.

Cloudfare est toujours là. Ils nous ont dit qu'ils le feraient à travers l'algorithme ECDSA et ça me fait réfléchir à si les gens vont l'utiliser et à si on pourra le voir dans leurs ensembles de données.

Donc, en fait, en résumé, pourquoi utiliser l'ECDSA, quel est l'intérêt ? Si vous ne l'utilisez pas, pourquoi devriez-vous changer et vous y mettre ?

Le DNSSEC a des problèmes de capacité parce qu'il est fragmenté. Oui, c'est toujours le cas en 2017, malheureusement, et ça ne changera pas, toujours malheureusement.

Le deuxième problème est que le DNSSEC fait l'objet d'abus pour des attaques d'amplification, et ça dépend du type d'attaques, de si l'amplification est l'attaque du jour, ou si les personnes utilisent d'autres méthodes. Mais il y a beaucoup de rapports disant que certaines attaques d'amplification principale utilisaient ces domaines. Ça a été le cas aussi il y a quelques semaines.

La cause commune est le fait que le DNSSEC a des messages très longs, qui sont longs parce qu'ils contiennent des signatures et des clefs RSA.

La solution est d'utiliser la cryptographie de courbe [inaudible], parce qu'on a des clefs plus courtes, des signatures plus courtes, et des sécurités cryptographiques plus fortes. En fait, vous avez tous ce qui se fait de bien sur Internet en un seul algorithme.

Une fois cette étude sur l'intérêt de l'ECDSA faite, les gens ont commencé à l'adopter. On a collecté des donnés à travers différents logiciels et à travers une initiative appelée Open Intel, dans différents laboratoires qui fonctionnent en réseau. Il s'agit d'une plateforme d'enregistrement de DNS à grande échelle. Si Open Intel vous intéresse, je pourrai vous en parler plus après cette réunion.

Donc, on a fait des enregistrements pour .NET, .COM, et .ORG, les principaux TLDs, jusqu'au 14 février de cette année. Pour .NL, on a eu des données sur un an environ. Ensuite, pour .GOV, un TLD très particulier, on a eu des données pour un seul jour. Et on a également évalué, à ce jour, des données pour six autres ccTLDs, certains étant d'ailleurs de cette région.

Dans ce tableau – les diapos sont disponibles sur le site ICANN, vous verrez les statistiques. Il n'y a différents degrés d'adoption du DNSSEC. .NL a les valeurs les plus élevées en termes relatifs

pour ce domaine, tout du moins par rapport à l'ensemble des données évaluées. Je pense qu'en Norvège, le pourcentage est un peu plus haut. Mais pour .NL, ça atteint presque 50%.

Dans cette autre diapo, je montre la méthodologie. On voulait voir l'adoption de l'ECDSA. On a évalué et analysé les identificateurs d'algorithmes dans le DS, la clef DNS et le RSSAC. On a fait la distinction entre les déploiements complets et partiels. Donc, si on avait la clef DNS, on devait voir s'il y avait dans le DS une délégation sécurisée, et s'il y avait un déploiement complet avec RSSAC.

Ici, on a le graphique des trois plus grands gTLDs. Comme vous le voyez, le graphique commence en octobre 2015, parce qu'avant cette date, il n'y avait presque pas d'adoption. Ce que vous voyez dans le graphique, ce sont les dates auxquelles Cloudflare a annoncé le DNSSEC universel. Pendant un an à peu près à compter de cette date-là, Cloudflare a été la seule source de déploiement significatif du DNSSEC dans .COM, .NET et .ORG.

C'est aussi intéressant de savoir que le déploiement complet est en bleu foncé, et que le bleu clair correspond au déploiement partiel. Malheureusement, personne ne peut valider les signatures dans les cas en rouge.

À partir d'avril 2016, c'est très difficile à voir dans cette diapo, mais quelqu'un a commencé à signer ses domaines avec

l'ECDSA. Il s'agit d'une société de média qui publie de nombreux journaux aux États-Unis, des publications mondiales comme le *Sacramento Bee*.

Puis, ça a commencé à vraiment s'accélérer à partir de la mi-octobre de l'année dernière lorsque. Domainnameshop, une société norvégienne - à qui j'ai demandé la permission de les citer ici parce qu'il fallait qu'ils soient d'accord – et Domainnameshop a donc adopté l'ECDSA pour tous les domaines qu'ils ont signés. Je pense qu'ils signent tous les domaines par défaut s'ils utilisent leur serveur, ce que fait la plupart des gens, c'était donc intéressant de voir qu'ils ont commencé à utiliser cet algorithme.

Ils signaient avec RSA avant, et à cette date-là, j'ai vérifié, ils ont commencé à signer avec l'algorithme ECDSA. Ils ont d'abord publié les signatures, puis les chiffrements, ils ont eu les deux, RSA et ECDSA qui ont coexisté pendant un mois, puis ils ont complètement changé pour l'ECDSA. Actuellement, leur déploiement est beaucoup plus important que celui de Cloudflare.

Je me suis plutôt concentré sur l'adoption partielle parce que ce type d'adoption se fait non seulement pour l'ECDSA, mais aussi pour d'autres algorithmes.

À gauche sur cette diapo, on voit l'adoption des RSA 1 et 6.3, l'algorithme 7 donc, et ce que vous voyez ici est le fait que c'est presque exclusivement pour le déploiement. Sur la droite, on voit le taux d'adoption de RSA 2.6 et 6.3 où la plupart des déploiements sont partiels. C'est-à-dire que beaucoup de gens font signer leur domaine mais sans avoir de délégation sécurisée.

On a essayé de se renseigner pour savoir pourquoi cela se produit et ça varie, en fait. Parfois, le bureau d'enregistrement ne soutient pas les délégations sécurisées ou bien ne fournissent pas de soutien pour ces algorithmes, ou alors les titulaires de noms de domaine oublient d'enregistrer leur délégation sécurisée. Et tous ces facteurs surgissent en même temps.

On espère que pour l'utilisation de clef ECDSA cela va changer, parce qu'il pourrait y avoir un référentiel de domaine signé dans les TLDs tel que .COM qui, en ce moment, ne peut pas être validé parce qu'il n'y a pas de délégation sécurisée. Cela augmenterait le déploiement ECDSA dans ces TLDs de manière substantielle.

J'ai déjà tweeté cette image mais j'ai préparé le graphique en forme de camembert de la distribution de l'algorithme de .COM et voit très rapidement que le P 256 du ECDSA va adopter l'algorithme numéro 8, ce qui est tout à fait intéressant. Il paraîtrait que ces nouveaux déploiements de DNSSEC

commencent de plus en plus à utiliser l'ECDSA plutôt que le RSA, et ce dès le départ.

Ce qui nous inquiète, c'est qu'un grand pourcentage de personnes utilise toujours les versions SHA-1 et NSEC3 qui suivent les annonces de SHA-1. Je ne sais pas qui a dit qu'il y aurait des discussions là-dessus lors de l'IETF à Chicago, est-ce bien le cas ?

DAN YORK : Quelqu'un a une version préliminaire de l'ordre du jour ?

ROY : Il y a eu deux versions préliminaires publiées. Paul [inaudible] et moi-même avons élaboré deux versions préliminaires pour discuter des mises à jour des algorithmes SHA-1 et NSEC 3 entre autres.

DAN YORK : Oui, mais l'idée serait d'encourager les gens à migrer au SHA-256 et à ne pas utiliser le SHA-1.

ROY : Exactement.

[ROLAND VAN RIJSWIJK]: Bien. Diapo suivante.

Je ne peux pas m'empêcher, et je dirais que l'ECDSA pourrait être encore mieux et renforcé, il pourrait être énorme. Vous pouvez me haïr, mais c'est vrai que ça pourrait être énorme parce que si tous les noms de domaine opérés par Cloudflare déployaient le DNSSEC universel, ça ferait plus que doubler la quantité de noms de domaine dans .NET et .ORG, et du jour au lendemain, ça ferait de l'ECDSA l'algorithme le plus utilisé dans le .COM.

Je vais laisser à Oliver le temps de prendre des photos, je peux vous passer la diapositive si vous la voulez. Je pense qu'Oliver a déjà dit que Cloudflare a une politique selon laquelle les gens doivent décider consciemment d'enclencher le DNSSEC plutôt que de le faire par défaut pour leurs clients. Ce type de politique est commune à notre cas. Avec Surfnet, on ne peut obliger personne, on veut voir ce type de croissance organique dont on parlait tout à l'heure, les gens doivent décider de le faire. Mais si le tout le monde le faisait et pouvait être encouragé à le faire, Cloudflare pourrait être aussi énorme que les autres.

On a également vu l'adoption dans le ccTLD .NL qui est le ccTLD qui a le plus de nouveaux gTLDs adoptés, mais le .NL ne supportait pas les délégations sécurisées jusqu'en mars de l'année dernière. Donc, on voulait voir si on pouvait avoir un

effet sur les ensembles de données. On a vu l'impact ici pour les gTLDs signés avec le .NL à travers Cloudflare avec délégation sécurisée. Si vous regardez les flèches en haut, elles disent que plus de 50% de cette délégation partielle qui existaient avant la délégation sécurisée en sont toujours au point de départ, en délégation partielle cette année.

La conclusion est donc que les gens oublient. Elles enclenchent le DNSSEC puis elles oublient de faire la délégation sécurisée. J'ai regardé comment les gens avaient enregistré leur délégation et, en principe, elles voulaient le déployer. Elles pourraient faire une déploiement complet puisqu'elles avaient commencé le processus.

Ce qu'on voit d'autre ici est que seuls les noms de domaine de Cloudflare opèrent avec l'algorithme ECDSA, puis à partir de juin 2016, il y a eu d'autres opérateurs qui ont commencé à l'utiliser. C'est à ce moment qu'on a lancé le Power DNS 4.0 qui utilisait l'algorithme ECDSA comme algorithme par défaut.

On voit également des hôtes hollandais locaux qui ont également commencé à utiliser l'ECDSA pour leurs noms de domaine signés.

Si vous prêtez attention, vous verrez que sur la gauche, on parle de 8000 domaines signés avec l'ECDSA. Si vous y réfléchissez,

presque 2, 6 millions de délégations ont été signés dans le .NL. C'est donc un petit chiffre, un petit pourcentage.

Pourtant, les gens du .NL ont montré qu'il est possible de faire un roulement avec le nouvel algorithme sans casser le système. Je ferai le roulement en direct et je ferai un article de blog là-dessus pour tout montrer aux clients et aux gens.

On a également analysé six autres ccTLDs, l'Autriche, le Canada, le Danemark, la Finlande et la Suède.

Ici, ce qu'on voit est que, par exemple, Alexander de .AT a dit ce matin qu'ils viennent à peine de commencer à supporter la délégation sécurisée pour leur ccTLD, ce qui est reflété dans la quantité de noms de domaines ayant adopté l'ECDSA, à savoir seulement 1% du total.

Mais dans le cas dans le Finlande, c'est 75%, au Danemark, 88% des noms de domaines signés utilisent l'ECDSA. C'est probablement parce que ce sont des déploiements plus récents où les gens analysent tous les documents et se disent « je veux déployer le DNSSEC et le faire de manière moderne, donc j'utiliserai un algorithme qui ne donnera pas d'énormes réponses à mon DNSSEC ».

Diapo suivante. Par la suite, on a analysé le .GOV. Les organismes fédéraux doivent signer leur nom de domaine

enregistré sous le .GOV. En 2009, il a été édicté que les noms de domaine fédéraux devaient être signés et il est recommandé aux organismes d'utiliser l'algorithme ECC et de s'assurer d'utiliser des clefs plus longues. Donc, nous nous sommes demandé si les noms de domaine .GOV utilisaient l'ECDSA et la réponse est non, aucun ne l'utilise. D'autres faits curieux...

INTERVENANT NON IDENTIFIÉ : Il est impossible de mettre à jour les clefs ECDSA en raison du registre .GOV.

[ROLAND VAN RIJSWIJK]: D'accord, je ne savais pas. Ça fait mal.

Donc, un fait curieux : 8% des noms de domaine .GOV des RSA de 1024 bits. Paul disait qu'ils ne remplaçaient pas les dispositifs. Six noms de domaine .GOV utilisent toujours des RSA de 512 bits et presque 50% des domaines .GOv utilisent SHA1 en dépit des recommandations de [inaudible] de ne pas le faire en 2015. Paul dit qu'ils ont des anciennes imprimantes.

ROY : C'est parce que leurs outils de déploiement ne sont pas faciles à utiliser.

[ROLAND VAN RIJSWIJK]: Ce n'est pas une excuse.

Donc, où en est .GOV ? Pour ce qui est de l'une des premières initiatives de déployer l'ECDSA dans l'espace gouvernemental, ils sont véritablement en retard. Ça nous inquiète. Je n'ai pas discuté avec Scott Rose de cette question mais j'imagine qu'il n'est pas content là-dessus.

DAN YORK : On lui demandera la semaine prochaine à Chicago, s'il est là.

[ROLAND VAN RIJSWIJK]: D'accord. Je ne serai pas là mais demandez-lui si vous le voyez.

DAN YORK : Sans doute.

[ROLAND VAN RIJSWIJK]: Ce n'est pas qu'on veut se moquer du .GOV. C'était une bonne initiative au départ, mais ça vous montre aussi qu'il faut toujours faire attention, si vous faites le DNSSEC. C'était une technologie toute neuve au moment du déploiement et avec l'utilisation de l'ECDSA et l'introduction d'autres algorithmes, la technologie est obsolète mais il faut être toujours à jour, si ça vous intéresse, c'est le cas aussi avec la technologie DANE.

DAN YORK : Oui, du point de vue cryptographique, certains voudraient avoir des sécurités renforcées, parce que le niveau de sécurité est plus élevé qu'auparavant. Ça prendre encore plus de temps de faire migrer ces sites .GOV vers quelque chose de plus avancé que l'ECDSA.

[ROLAND VAN RIJSWIJK]: Oui. C'est vrai. Au départ, on a montré que la signature avec une ZSK, une clef de signature combinée avait d'autres avantages pour la réduction de la fragmentation et la lutte contre l'amplification. Comme les réponses du KSK sont les réponses les plus spécifiques à être fragmentées dans le DNS pour avoir des réponses plus longues qui utilisent l'amplification, l'idée est de réduire la taille de ces réponses à travers l'ECDSA, ou même à travers le EDDSA une fois qu'il sera disponible dans sa mise en œuvre. On pourra réduire la taille sensiblement, mais l'utilisation d'une seule clef de la moitié de la taille qu'on avait avant va aussi avoir un impact.

Donc on s'est demandé si les gens utilisent des clefs combinées avec l'ECDSA, et malheureusement on n'a pas réussi à trouver de tendance claire. Il y a un peu de tout, et dans certains ccTLDs, il y a des quantités de noms de domaine qui utilisent ce type de clefs de signature combinées, et dans le cas d'autres comme dans

.ORG, il n'y a pas d'évidence d'adoption de ce type de clefs combinées.

Si vous n'avez pas envisagé ça, je pense que vous devriez le faire. Je pense que le Power DNS utilise une combinaison des deux par défaut. Donc Power DNS a des utilisateurs qui utilisent l'ECDSA et ce sera fait à travers ce schéma de clefs combinées et de KSK.

Pour l'ECDSA, il est également intéressant de revenir en arrière et de voir quels sont les accomplissements atteints depuis. 1024 bits sont considérés un mode de sécurité trop faible de nos jours. On recommande de migrer vers des clefs plus fortes et on se demande si les gens le font. Si on regarde les chiffres pour .NET, .COM et .ORG, dans ces trois cas, 40% des DNS qui utilisent ce type d'enregistrement utilisent 1024 bits. Ces quantités sont substantielles mais il manque beaucoup d'enregistrements. Il faut prendre des mesures pour résoudre cela.

Les gens semblent croire que les clefs RSA ne viennent qu'en 1024 bits, il faut donc les informer pour qu'ils sachent comment se mettre à jour. Si vous avez 1024 bits, il faudrait migrer vers 2048, et si vous avez 2048, migrez vers 4096.

Combien de gens qui ont le RSA ont une clef d'une taille qui n'est pas aussi lourde ? Dans le cas du .NL, ce n'est pas négligeable mais c'est tout petit.

Si vous ne pouvez pas migrer vers l'ECDSA et que vous êtes coincés sur RSA mais que vous avez besoin de faire augmenter vos mesures de sécurité, les clefs combinées pourraient vous aider et être plus sensibles au moment de gérer la quantité de réponses. C'est une idée toute simple.

Diapo suivante. On a parlé de l'EDDSA, c'est quelque chose de très récent qui a été normalisé. Il y a deux courbes, ED 25519 et ED 448. Je veux dire que c'est vraiment très intéressant pour le DNSSEC, parce que la clef nécessite seulement 32 octets dans un enregistrement de clef DNS. Cela veut dire qu'il vous faut 64 bits. L'EDDSA utilise une autre partie de la représentation de la courbe, cela veut dire qu'on peut stocker des clefs encore plus petites.

L'ED 448 a aussi été normalisé comme étant une courbe vraiment solide. Si vous voulez vraiment avoir un niveau de sécurité très élevé, avec 224 bits de sécurité pour cet algorithme. Je pense qu'avec une courbe à 448 bits, vous êtes bien.

Comme l'EDDSA est nouveau, il n'existe pas de logiciel. Mais l'EDDSA est beaucoup plus rapide que l'ECDSA. Il faut moins d'espace et il a de meilleures propriétés en matière de sécurité. Bruce et ses collègues ont de bonnes listes des propriétés qui nous donnent la différence entre ces deux courbes en matière de propriétés.

Ce que je veux dire, ce que vous demandiez aux gens de soutenir la mise en œuvre de l'EDDSA dans les logiciels à code ouvert. Nous renouvelons notre infrastructure DNS pour stocker les clefs. J'encourage nos fournisseurs à adopter ces courbes dans leurs propositions commerciales. Il paraît qu'ils sont assez preneurs.

Prochaine diapositive. Pour conclure, le graphique vous a montré que l'adoption de l'ECDSA commence à croître et on voit un nombre significatif de domaines signés avec cet algorithme. Mais le déploiement ne concerne qu'une centaine d'opérateurs. On voit qu'il y a croissance, mais cela concerne 5 opérateurs importants. Il y a aussi d'autres opérateurs qui utilisent RSA 1024 bits. Le déploiement du DNSSEC se fait de manière assez générale et, en général, en adoptant l'ECDSA.

Alors, si vous êtes opérateur DNSSEC et que vous envisagez un nouveau déploiement, je vous recommande d'utiliser l'ECDSA PT56. Même si c'est toujours un risque, les gens disent que c'est tout à fait possible et nous allons le faire en 2017.

Si vous faites validation de DNSSEC, je vous encourage à utiliser l'ECDSA, 85% des opérateurs utilisent cet algorithme et nous encourageons son utilisation.

Nous allons passer à l'ECDSA PT56 en 2017. Nous allons combiner les clefs pour tous les domaines que nous signons pour

nos clients. Nous allons migrer vers un nouvel HSM. Il y aura beaucoup de domaines signés comme ça. Il y a de petits opérateurs et nous allons essayer de partager nos expériences.

Nous allons donc partager les scripts automatiques, le code, pour que les gens puissent s'en servir. Nous allons également partager les scripts avec le DNSSEC ouvert.

Si vous avez déjà déployé le DNSSEC ouvert, je vous recommande de l'utiliser parce que cela permettra de migrer vers un nouvel algorithme et ce sera plus facile de le faire.

Ensuite, diapo suivante, voici pour référence certains documents que vous pouvez lire. Il y a aussi des liens.

C'est tout. Je tiens à remercier les gens qui travaillent sur le projet SDIN. Je suis prêt à répondre à vos questions.

DAN YORK : Tout d'abord, je veux te dire merci pour ces informations. Merci pour ce travail, c'est vraiment très intéressant.

Je vois Paul, Jacques, Peter et d'autres qui souhaitent prendre la parole.

PAUL : Une des diapos disait que l'EDDSA était plus rapide, je suppose que c'est pour signer que c'est beaucoup plus rapide ?

[ROLAND VAN RIJSWIJK]: Les deux sont rapides pour signer. Si vous me donnez une minute, je peux vous donner les chiffres.

PAUL : C'était ma deuxième question. Vous avez bien montré pourquoi l'ECDSA n'était pas si [pénible]. Avez-vous des chiffres pour l'EDDSA ?

[ROLAND VAN RIJSWIJK]: Attendez, je cherche. J'espère que j'arriverai à trouver le lien. Oui.

Alors, ED25519, en termes de vitesse de validation, si l'on compare avec le SSL ouvert, à 1.L.2., cela nécessite 70% du temps du CPU pour être validé. C'est donc 30% plus rapide. Er pour l'ED448, c'est deux fois moins rapide que le .6. Si on compare à ED448, c'est quatre fois plus rapide. Cela vous donne beaucoup plus de sécurité.

DAN YORK : C'est un choc.

INTERVENANT NON IDENTIFIÉ : C'était une bonne présentation. Je me demande si on a des statistiques par rapport aux TLDs qui ont été signés avec

l'ED, parce qu'avec EC, on en a beaucoup, mais avec ED, avez-vous les statistiques pour savoir quels domaines ont été avec ?

CARSON : Carson de [inaudible]. Merci beaucoup pour cette présentation, Roland.

La dernière fois que j'ai changé les algorithmes, c'était l'année dernière. Je voulais donc savoir où en sont les logiciels par rapport à ces changements d'algorithmes ? Peuvent-il les supporter ? Parce qu'actuellement, ce n'est pas impossible mais c'est très difficile de le faire.

DAN YORK : Andre ?

INTERVENANT NON IDENTIFIÉ : Je parlerai d'abord parce que j'étais plus proche du micro.

Je profite de cette occasion pour essayer de vous encourager à faire quelque chose.

Alors, on utilise des logiciels, et les gens nous posent des questions. Par exemple, « est-ce que vous pouvez faire un roulement KSK en ajoutant une clef dans les lignes de commande, puis faire une ligne de commande pour éliminer

l'ancienne clef ? ». Manuellement, on pourrait le faire. Et nous aimerions que cela soit amélioré, c'est sur notre feuille de route.

Est-ce que vous savez combien d'hébergeurs ont soutenu notre programme de développement ? C'est pareil que pour l'ECDSA au niveau du gouvernement, c'est zéro, nul, rien.

Nous parlons toujours des opérateurs en disant qu'ils ne sont pas assez rapides, mais il faut aussi parler des hébergeurs. Il faudrait donc voir que lorsqu'on demande aux gens de développer ce type de choses, on n'obtient pas autant de réponses que l'on voudrait.

Alors, pour pouvoir changer les choses, j'aimerais beaucoup automatiser ce processus. Ce ne serait pas difficile, mais il faut que les gens puissent contribuer au niveau des efforts, au niveau des coûts.

Je lance donc un appel à tous ceux présents dans la salle pour soutenir le développement de logiciels.

DAN YORK : Très bien. Vous devez donc encourager, toujours, les gens à contribuer. On peut contribuer avec des codes ou avec des fonds.

Peter ?

PETER : Peter [inaudible]. Je veux remercier Roland pour son excellente présentation et pour son travail.

Une ou deux questions ou remarques. Tout d'abord, bien sûr, il y a des différences intéressantes entre one K et two K, et on voit que les gens pensent en termes de puissance 2. Quand vous parlez de la clef combinée, est-ce que ce ne serait pas possible d'avoir une ou deux clefs combinées ? Parce que, finalement, c'est la force du système dont on parle.

[ROLAND VAN RIJSWIJK]: Je ne sais pas pourquoi on le ferait, mais très peu de gens utilisent des clefs combinées. Je n'ai pas vu de déploiement par rapport à cela. En général, on utilise des clefs à 64 bits.

IDENTIFIANT NON IDENTIFIÉ : Je me demandais pourquoi le séparer quand les bureaux d'enregistrement auront tout entre les mains, y compris les clefs pour le système d'enregistrement ? Maintenir le RSA...

[ROLAND VAN RIJSWIJK]: Parce que nous leur avons dit dans notre RFC 4641 qu'il fallait les utiliser comme ça, les clefs.

INTERVENANT NON IDENTIFIÉ : Oui, mais la version mise à jour de ce RFC 6781 disait un peu la même chose. Mais pourrait-on combiner ces clefs ? Et si l'on commence à penser en termes de puissance 2, est-ce que le 248 pourrait modifier le trafic outbound ?

Du côté de l'ECDSA, je vois qu'il y a du soutien des fournisseurs pour ces nouvelles courbes. Nous avons fait un exercice l'an dernier et je crois que nous avons eu la même réponse : « Oui, oui, oui. Nous allons le faire ». Mais les fournisseurs nous ont dit que c'était beaucoup plus difficile que d'ajouter une autre courbe sur l'ECDSA parce qu'ils avaient déjà un système en place et il ne faudrait pas qu'ils perdent leur certification.

Ici, il y a le piège de la conformité, parce que si on nous demande d'utiliser un algorithme avec une certification donnée, à ce moment-là, on ne peut pas innover et ce n'est pas bien. Là se pose la question des régulateurs, des législateurs.

Vous avez parlé de l'EDDSA. Ce serait intéressant pour une partie du public qui n'a pas besoin d'avoir de randomisation, ils produisent des signatures dans des scénarios redondants. Ce n'est peut-être pas important pour la randomisation mais peut-être pour les installations plus importantes.

[ROLAND VAN RIJSWIJK]: Oui, il y a des problèmes de sécurité également. Je n'ai pas voulu rentrer dans le détail parce qu'il faut connaître un peu comment l'ECC travaille et c'est assez spécifique. Mais pour l'ECDSA, il y a deux mises en œuvre. On peut soit utiliser une chaîne randomisée, ça peut être complètement randomisée et alors il faut un moyen déterministe pour créer ces clefs. Si vous faites EDDSA, c'est la meilleure façon de procéder, parce que si vous générez deux signatures et que vous réutilisez les mêmes noms, alors votre clef privée ne peut pas être récupérée, et c'est un problème de sécurité très grave.

DAN YORK : Ce qui génère bien sûr un gros problème.

[ROLAND VAN RIJSWIJK]: C'est pour ça que je ne l'ai pas mentionné. C'est un problème très complexe.

DAN YORK : On sait que c'est très complexe. Alors, j'ai Erwin, puis Olivier. Est-ce qu'il a d'autres personnes qui veulent prendre la parole ?

Très bien. Erwin.

ERWIN : Je voulais confirmer les soupçons par rapport à ce qui a été dit. Si vous êtes un nouveau bureau d'enregistrement, vous utilisez l'algorithme 13. On est à près de 1% de domaines signés et ils ont fait un roulement d'algorithme.

DAN YORK : C'est assez intéressant de voir ce qu'un bureau d'enregistrement peut faire à ce niveau et faire un changement de ce type.

Oliver ?

OLIVER : Oui, Roland, c'était très intéressant et j'aimerais rebondir un peu sur ce que tu as dit et te taquiner un peu. Tu as parlé de mes clients, mais je voulais savoir si ce problème est important pour le reste du monde. Parce que si ces domaines sont gérés par des non-bureaux d'enregistrement, cela représente un problème.

[ROLAND VAN RIJSWIJK]: Excusez-moi si vous avez pensé que je vous taquinais, ce n'était qu'un exemple.

OLIVER : Oui. Nous essayons d'adopter un nouveau protocole dans le domaine des registres pour qu'ils puissent parler avec les bureaux d'enregistrement pour obtenir ces informations et

pouvoir les télécharger de manière normalisée, que tout le monde puisse le faire de la même manière. Voilà. Maintenant, on voit qu'il y a une adoption peut-être partielle bientôt.

DAN YORK : On a besoin de quelqu'un qui puisse s'investir dans du développement de code. C'est du code, finalement. Le code que crée le DNSSEC, c'est un code dont [inaudible] pourrait nous parler puisqu'il a travaillé là-dessus et nous sommes ouverts à l'extension de cela. C'est une question de temps pour certaines personnes qui n'en ont pas suffisamment pour se pencher là-dessus.

Très bien. Des questions ?

INTERVENANT NON IDENTIFIÉ : J'ai une question. Je ne sais pas, et j'aimerais savoir, par rapport à l'utilisation concrète comment je peux signer ma zone avec l'EDDSA et qu'est-ce qui se passe si le résolveur ne peut pas comprendre cette signature ? Que se passe-t-il à ce moment-là ? Dit-on au client que ce n'est pas authentifié ? Quel est le comportement attendu ? Ou bien il y a quelque chose qui se casse ?

DAN YORK : Si le résolveur ne connaît pas l'algorithme, il renverra une réponse non signée.

[ROLAND VAN RIJSWIJK]: Les gens de l'APNIC et Jeff se sont penchés sur cette question et ils ont trouvé que ce comportement est effectivement ce qui se produit. Il n'y a rien qui se casse parce qu'il y a une réponse non validée au final.

DAN YORK : Il y a une liste de diffusion. Je crois que quelqu'un avait dit avoir fait un roulement et des résolveurs configurés n'étaient pas bien configurés, et ils ont eu deux versions du DNS mask. Et donc le DNS n'avait pas été mis en œuvre de la manière dont le RFC l'indique. Cela s'est produit, cela a été réparé depuis, mais à ce moment-là, on a pu observer ce comportement.

Ensuite, nous parlons beaucoup de l'EDDSA. Une question rapide. Je vous regarde, Benett. Où en êtes-vous pour que cela soit disponible pour outbound ?

BENETT : Ce sera mis en œuvre bientôt. C'est sur le RFC. Ce sera disponible dans les librairies de sécurité bientôt. Oui, bientôt.

Ce matin, on avait dit qu'on attendait le soutien de cette mise en œuvre mais qu'elle est prévue pour dans pas longtemps.

DAN YORK : Très bien. D'autres questions ?

Très bien. Alors, je veux remercier Roland pour son travail.

Maintenant, si vous pensiez que nous étions déjà rentrés dans le cœur de monde des geeks, je vais vous présenter le questionnaire sur le DNSSEC.

JULIE : S'il vous plaît, je vous prie de regarder les réponses à ce questionnaire. Si vous n'avez pas de document sur votre chaise, vous pouvez chercher une feuille. On va vous donner des instructions sur ce que vous allez faire.

Nous aurons la pause déjeuner juste après le questionnaire. Nous vous avons donné des tickets pour le déjeuner. On vous attendra, il faudra remettre ces tickets pour pouvoir manger. Regardez autour de vous si vous avec vos tickets, parce qu'il y en a encore sur les chaises.

Donc, je vous prie de prendre les documents. Voilà.

WES: Comment de gens ont fait le questionnaire à Hyderabad ? Combien de gens ont eu des résultats négatifs ? Très bien. Alors, vous serez contents de voir que, cette fois-ci, il n'y a pas eu de résultats négatifs. Ce n'étaient que des résultats positifs.

Quelques règles rapides. Pour être gagnant, quelqu'un d'autre que vous doit pouvoir valider vos réponses. Chaque réponse correcte rapporte un point. Il y a plusieurs réponses correctes, mais si vous choisissez une réponse incorrecte, vous aurez zéro. Parfois, il y a plusieurs réponses correctes. Cela peut être bon ou pas. Ça dépend de ce que vous choisissez. Enfin, moi, Wes [Wardeker ?], j'ai toujours raison, y compris quand je suis malade, comme c'est le cas en ce moment. Ce que je dis est la vérité.

Question zéro : quel chocolat est disponible au Danemark mais est illégal à l'importation aux États-Unis ? Est-ce que c'est Kinder Surprise, Kinder Surprise, Kinder Surprise ou Kinder Surprise ? Vous pouvez avoir un prix si vous gagnez. Ce chocolat est extrêmement dangereux, cet œuf en chocolat est très dangereux et ne peut pas être importé aux États-Unis. Si vous gagnez, vous l'aurez. S'il y a égalité avec quelqu'un d'autre, vous devrez vous battre pour l'avoir.

Alors, vous voyez, 4 réponses correctes, A, B, C, D, ce qui ferait 4 points. C'est joli, n'est-ce pas ?

Première question, maintenant. Alors, première question. Lesquels de ces ccTLDs ont validé complètement le DNSSEC en décembre 2016 ? Oui, Peter ?

PETER : Je peux poser une question ? L'un d'entre eux se trouve sur la liste IETF des noms spéciaux ?

WES : [Pluton]. Hong Kong, Afrique du Sud, Vietnam. .HK, .ZA et .VN. Et bien sûr, [Pluton].

Question numéro 2. Où s'est tenue la première cérémonie de création de la première clef racine ? Était-ce à El Segundo, Californie, à Culpepper, Virginie, à Paris, France ou sur Pluton ?

C'est un thème général pour les prochaines questions. Puisqu'on va bientôt faire le roulement de la clef KSK, il y aura plusieurs questions sur ce sujet.

Très bien. Question numéro 3. Quand est-ce que la clef KSK actuelle sera révoquée ? Le 11 Juillet 2017, le 11 décembre 2017, le 11 janvier 2018 ou le 13 janvier 2018 ? C'est l'une de ces dates. C'est le moment où la KSK actuellement en vigueur sera révoquée, c'est-à-dire qu'elle ne sera plus valable.

Question numéro 4. Quel est le délai minimum pendant lequel l'ICANN doit attendre après avoir publié la nouvelle clef dans la racine du DNS pour que les validateurs conformes au RFC 5011 puissent avoir confiance dans la nouvelle clef ? Voilà. 30 jours, 45 jours, 61, 5 jours ou 365, 25 jours ? C'est le délai pendant lequel l'ICANN doit attendre pour que tous les validateurs DNSSEC acceptent la nouvelle clef.

Question numéro 5. Quelles sont les propriétés de la zone racine signée DNSSEC ? Est-ce A - nsec avec RSA SHA-1 et ZSK à 1024 bits ? B - nsec avec RSA SHA-256 et ZSK à 2048 bits ? C - nsec 3 avec RSA1 et ZSK à 1024 bits ? D – nsec 3 avec RSA SHA-1 et ZSK à 2048 bits ? E – TLS 3 V1, K V 2 pop 3 ?

Question numéro 6. Lesquels des ccTLDs suivants ont des enregistrements DS dans la zone racine ? Et vous avez plusieurs options - A, B, C, D, E. Par exemple, .AE, .BG, .CC, .DK, .AF, .BH, .CR. DK. Vous connaissez tous ce type de ccTLDS. Ou bien .WW, .XX, .YY, .ZZ. Vous savez que ça n'existe pas mais vous pouvez choisir cette réponse.

Pas d'ordinateur et on ne regarde pas sur les copies des autres, ce serait de la triche. Il ne faut pas tricher.

Très bien. Cinq... Quatre... Trois... Deux... Un...

Question numéro 7. Ici, vous obtenez beaucoup de points si vous avez la bonne réponse. Écrivez le nom d'un DNS ou d'EDNS enregistré avec l'IANA, aussi bien l'abréviation à deux caractères ou le nom enregistré. Par exemple, ça peut être DNSSEC OK ou DO. C'est la question numéro 7. Il reste une question, mais je vous donne quelques minutes pour écrire cette réponse.

Ensuite, question numéro 8. Quels sont les identificateurs de clef à cinq chiffres de clef active aujourd'hui dans la zone racine ? Tout le monde sait ça, non ? Vous pouvez le deviner, si vous voulez, c'est un numéro à cinq chiffres. Il y a une seule clef activée pour le ZSK. C'est la clef de signature.

Très bien, je reviens à la question numéro 7, pour que vous y réfléchissiez, et la question 8 était la dernière.

J'ai été malade hier soir pendant que je faisais ça, donc j'espère que ça va bien se passer.

On est revenus sur la question numéro 7 pour que vous puissiez la lire. On n'a pas de question 7, la dernière question est la question 8.

Deux lettres, oui.

Merci, Paul. Alors, je précise que pour cette question et pour celle qui porte sur l'identification de clef, vous pouvez deviner et si vous vous trompez, vous ne validerez pas le reste des

réponses. Donc si vous avez mal répondu à trois de ces réponses, et si vous écrivez AQ pour [inaudible], c'est bien, vous pouvez le noter, pas de pénalité.

Paul et Roy sont encore en train d'écrire, on leur donne une petite minute.

Il y a eu une expansion de sigle qui m'a surpris, parce que ça m'a pris du temps de trouver ces deux lettres dans les deux mots, en fait.

Allez, Roy, pressez-vous. C'est bon ? Paul, vous arrêtez. Je pense qu'on a fini. Julie, on avance ? Rappelez-vous que pour pouvoir participer au prix, il faut que vous passiez vos réponses à quelqu'un d'autre pour qu'il vous corrige, que ce ne soit pas votre femme ou votre mari, puisqu'on ne veut pas de triche. À la fin, je demanderai, au moment des qualifications finales, qui a corrigé votre questionnaire.

Bien, on avance. Julie. Question zéro, si vous avez demandé que c'était Kinder Surprise, vous avez les quatre points. Félicitations. J'espère que vous avez tout noté comme je vous ai dit de le faire.

Question suivante. Lesquels de ces ccTLDs sont complètement conformes au DNSSEC depuis décembre 2016 ? Ce sont les trois premiers. Pluton, bien sûr, vous donne zéro à toute la question.

Ma copie disait que ça datait de décembre.

Rappelez-vous que j'ai dit que c'était toujours moi qui avais raison, donc ça ne m'intéresse pas. Je vous donnerai le crédit pour les trois, mais de toute façon, mes fiches disaient décembre.

DAN YORK : Oui, vous avez raison. C'était le 16 décembre.

WES : J'ai toujours raison, je vous l'ai dit.

DAN YORK : Est-ce qu'on peut avancer parce que ça nous empêche d'aller manger ?

WES : Oui, j'aime faire ça avant la pause déjeuner, comme ça personne ne remet quoi que ce soit en question de ce que je dis.

Donc, la première cérémonie de signature de clefs a eu lieu à Culpepper.

Question numéro 3. La KSK actuelle sera révoquée le 11 janvier 2018.

Question 4. Quel est le délai minimum pendant lequel l'ICANN doit attendre après la publication de la nouvelle KSKS de la racine DNS pour que tous les validateurs conformes au RFC 5011 en ligne fassent confiance à la nouvelle clef ? 61 jours et demi.

WARREN : Non, ce n'est pas le cas. Ça dépend du fait que les validateurs soient en ligne.

WES : Non, non, j'ai ajouté ce détail. On dit « pour les validateurs en ligne ».

Question suivante. Question numéro 5. Quelles sont les propriétés correspondant à la zone racine signée DNSSEC aujourd'hui ? C'était la réponse B - ZSK et RSA SHA-256 à 2048 bits.

Question suivante. Quels ccTLDs parmi ceux qui suivent ont des enregistrements DS dans la racine DNS ? C'était la réponse A - AB, BW, CN et DK. Vous voyez, tous ceux qui sont en rouge et barrés ne le sont pas.

CN a un enregistrement DS. Est-ce que ça a été révoqué ?

DAN YORK : Ici, on dit décembre 2015.

WES : L'écran de Warren vient de me montrer que ça existe, en fait.

Warren, qu'est-ce que disait la deuxième diapo ? Pour rappel, j'ai toujours raison.

Je ne sais pas, c'est un problème avec votre résolveur.

INTERVENANT NON IDENTIFIÉ : Concentrez-vous, Warren, on veut manger.

WES : Écrivez tous les DNS et EDNS enregistrés à l'IANA ? Pas besoin des valeurs, je vous donne ici les réponses. AA, authoritative answer. TC, truncated response. Si vous avez écrit trancated autre chose, même si response n'a pas de C. La réponse est truncated response TC. RD, recursion desired. RA, recursion available. AD, authentic data. Pas authenticated mais authentic. CD, checking disabled.

Et bien sûr, celui que je vous ai donné comme exemple, le DO pour DNSSEC OK.

INTERVENANT NON IDENTIFIÉ : Vous avez oublié une réponse. QR.

WES : C'est à l'IANA qu'il faut le dire, ça a été tiré de leur site Web.

J'ai pensé qu'il y en avait d'autres mais vraiment, c'est ce que j'ai copié sur leur site Web.

Question suivante. Les identificateurs de clef actuels. Est-ce qu'on peut revenir en arrière ?

DAN YORK : Allez, on voudrait manger.

WES : D'accord. J'accepte les deux réponses si vous n'avez pas ajouté le mot « answer » et que vous n'avez mis que DNSSEC OK, parce que c'est ce que j'avais dit au départ.

Question numéro 8. Les identificateurs de clef à cinq chiffres actifs dans les clefs de la zone racine aujourd'hui sont KSK 19036 et ZSK 61045. Est-ce que quelqu'un les a bien écrites ?

Bon, on a plusieurs réponses, il y en a des milliers qui sont incorrectes.

C'est tout ? Je pense que la diapo suivante est vide.

Alors, maintenant vous devez rendre les interros à vos partenaires. Calculez votre note. Est-ce qu'il y en a qui ont eu

moins de 5 ? Dans ce cas-là, vous n'avez pas suivi mes instructions. Vous avez des questions ? D'accord.

Donc, qui a eu plus de 8 ? Plus de 8 ? D'accord. Il y a plusieurs personnes. Qui a eu plus de 9 ? D'accord. Vous avez eu au moins 10 points. 11 ou plus ? De ce côté de la table, on a le panel d'experts. 12 ou plus ? 13 ? Plus que deux. Je vais chercher le petit chocolat.

Je les fais travailler. 14 points ? D'accord, je le donne à Paul et Warren, et c'est à eux de décider comment se partager ce chocolat. C'est interdit aux États-Unis parce que vous risquez de vous étouffer avec les petits jouets.

Merci et bon appétit.

DAN YORK : Le déjeuner sera servi dans la salle C.1.1. C'est au fond. Vous pouvez suivre les panneaux pour y arriver. Si vous n'avez pas de tickets et que vous voulez nous rejoindre, demandez-nous de vous en donner un.

Nous nous réunirons ici à 13 : 45. C'est ce qui est prévu, n'est-ce pas ? Donc revenez dans 40 minutes.

[FIN DE LA TRANSCRIPTION]