BARCELONE – Atelier sur les DNSSEC - (2 sur 3)
Mercredi 24 octobre 2018 – 10h30 à 12h00 CEST
ICANN63 | Barcelone, Espagne

JACQUES LATOUR : Nous allons bientôt commencer. Bonjour. Jacques Latour avec CIRA et nous avons donc Steve Crocker qui est avec nous par téléphone. Je vais m'occuper de ce panel.

Donc l'objectif de ce panel est de poursuivre une discussion que nous avons commencée à Johannesburg lors de la réunion 59 de l'ICANN. À ce moment-là, il y a eu une réunion politique et on a cet atelier DNSSEC, pendant lequel nous avons regardé quel était l'impact du CDS, CDNSKEY. Et la raison pour laquelle nous avons essayé de voir ce qui se passe là, c'est que, à l'époque, c'était en fait l'année dernière, lorsqu'on a commencé à réfléchir à l'idée de scanner toute une zone et de prendre le CDS et de l'importer dans les registres, plusieurs personnes ont dit possible, ce n'est pas possible parce que c'est en infraction avec les politiques de l'ICANN. Donc voilà pourquoi on avait organisé cette réunion. Et alors on s'est dit quelles sont les politiques en infraction.

Et enfin, personne n'a trouvé de politique qui était vraiment en infraction, mais on a commencé à faire des recherches savoir quelles étaient les politiques impactées ; y avait-il des politiques relatives au DNSSEC ? Et lorsqu'on a pris en compte l'accord de base des opérateurs de registres pour les gTLD, il est inscrit que l'opérateur de

registre acceptera des supports de « fille » conformément aux meilleures pratiques dans l'industrie.

Donc la méthode n'est pas clairement inscrite en termes d'infraction des politiques. L'accord de base avec les registres ne les empêche pas d'obtenir le DS de la zone « fille » directement. Pour ce qui est du RAA, donc, de 2013, l'accréditation des bureaux d'enregistrement, il est marqué que le bureau d'enregistrement acceptera ou plutôt traitera les informations DNSSEC en faisant passer les ordres de changement. Donc c'est faire passer les informations. Ce n'est pas stocker, ni traiter, ni garder les informations. Donc de ce point de vue, il ne me semble pas- en tout cas, nous sommes d'accord pour dire qu'il n'y avait pas d'infraction de l'accord parce que la prescription n'était pas très claire. Le détail n'était pas très clair. Donc maintenant, étant donné qu'il n'y a pas d'infraction au d'accord, nous avons plusieurs options et donc, Steve va nous parler de là où nous en sommes, des différentes options pour avancer.

Alors Steve, c'est à vous.

RUSS MUNDY : Vous m'entendez ?

STEVE CROCKER : Excusez-moi. J'avais éteint mon micro. Merci, Jacques. Merci à tous d'être présents pour ce panel.

Ce qui me préoccupe, c'est que ça fonctionne et je ne vois pas

exactement comment. Je vois qu'il y a beaucoup d'initiatives. Ces clés DNS, donc cette approche-là. Et si c'est ce qui fonctionne, eh bien, aucun problème de mon côté. Mais, pour l'instant, je n'ai pas encore pu constater un accord et une acception large du côté des registres gTLD et du côté des bureaux d'enregistrement également.

J'ai écouté les différentes démarches et il me semble qu'elles correspondent à un modèle très simple avec trois choix binaires. Alors diapositive suivante, s'il vous plait. J'ai un problème avec la distance, me semble-t-il.

RUSS MUNDY : Non, j'ai l'impression qu'il y a un problème avec Adobe, Steve. Je suis désolé, nous allons essayer de résoudre le problème.

STEVE CROCKER : Alors je vais faire comme je peux, parce qu'en fait je n'ai pas la présentation devant moi. Mais voilà un petit peu ce qui se passe. Avec la publication CDS CDNSKEY, il y a une attente comme quoi l'opérateur de registre va tirer l'enregistrement. Donc c'est le modèle tirer ou extraire. L'idée complémentaire, c'est que les nouveaux enregistrements sont repoussés vers le haut par une interface, quelle qu'elle soit.

Donc voilà un premier choix binaire : pousser ou tirer, pousser ou extraire.

Deuxièmement, soit on communique les enregistrements DS ou une

nouvelle clé, et l'enregistrement DS est calculé sur la base de cette clé.

Troisième choix binaire, est-ce qu'on roule le parent grâce au registre ou grâce au bureau d'enregistrement ? Donc on pourrait imaginer que le bureau d'enregistrement scanne la zone fille plutôt que ce ne soit l'opérateur de registre qui le fasse. Et le bureau d'enregistrement utilise l'interface pour le pousser, pour le communiqué au registre.

Ça y est. Je vois les diapositives. Alors on va passer à la diapositive suivante. C'est bon ? Est-ce que vous voyez ? Donc voilà toutes les options. N'importe laquelle pourra marcher. On peut d'ailleurs en utiliser plusieurs. Je sais que Switch utilise à la fois extraire et pousser, avec en priorité pousser me semble-t-il.

Diapositive suivante. Alors qui choisit ? Eh bien là, on peut en débattre. Diapositive suivante.

Donc, là, je m'adresse à ces intervenants lors du panel, donc ce que je souhaite c'est, soyez clairs par rapport à ce que vous faites, mais également soyez clairs par rapport à ce que vous souhaitez que les autres fassent.

Et il y a une question qui reste, à savoir est-ce qu'il y a quelque chose qui nous empêche du point de vue politique, du point de vue des contrats. Et si c'est le cas, eh bien, il faut absolument éclaircir la situation, s'en occuper de manière à ce que les choses soient réglées. Mais il faut être explicite. Il faut être clair par rapport aux informations du WHOIS. Je sais que ce n'est pas quelque chose qui plait, mais il faut absolument que les problèmes soient résolus. Voilà. Je repasse la

parole à Jacques.

JACQUES LATOUR : Nous venons de voir les diapositives, Steve. Elles viennent d'arriver. Alors est-ce qu'on pourrait passer à la diapositive numéro trois, s'il vous plait ? Les trois options, donc.

Je crois qu'il est important de bien comprendre ceci. Steve, peut-être que vous pourriez repasser en revue cette diapositive, de manière à ce qu'on puisse mieux comprendre. Steve, est-ce que vous pourriez nous représenter ces trois options ? Je pense que votre micro est éteint.

La clé, ce dont il faut absolument parler, c'est la question de savoir si on pousse ou si on extrait. On a KSK avec DS. Et en bas, nous avons donc le parent avec le registre ou bureau d'enregistrement. Donc en principe, on ne devrait pas avoir plusieurs choix ; on devrait simplement choisir une option que l'industrie utilisera.

MICHALE HAUSDING : Alors en ce qui concerne Switch, on a utilisé le modèle Push. Mais nous avons eu certaines complications et donc il semblerait que le modèle extraire soit plus facile à utiliser. Mais nous avons quand même le modèle pousser. Il est disponible. Si vraiment vous souhaitez changer quelque chose dans la zone parente, vous avez cette option.

Est-ce que vous voulez que je montre mes diapositives maintenant ? Sinon, je préfère en parler plus tard.

JACQUES LATOUR : Alors, nous allons maintenant passer la parole à Vicky.

VICKY SHRESTHA : Bonjour. Désolée, excusez-nous. Diapositive suivante s'il vous plait.

Donc je travaille sur les DNS à Cloudfare. Et nous gérons beaucoup de réseaux. Nous nous occupons également des résultats de validation du DNSSEC — diapositive suivante — dans le monde entier donc.

En ce qui concerne cette présentation, je vais parler du travail que nous avons fait sur le DNSSEC jusqu'à maintenant. Nous activons le DNSSEC pour tous nos clients depuis 2015. Nous avons fait la publication de CDS, CDNSKEY depuis assez longtemps. Nous avons également un soutien pour le CDS 0, et le CDNSKEY 0.

Beaucoup de nos clients essayent d'activer le DNSSEC, mais le problème, c'est qu'ils ne font pas le suivi. Donc ils activent le DNSSEC sur le bon portail, mais ils le laissent tel quel. Donc ils ne se retournent pas vers les bureaux d'enregistrement avec les mises à jour et ceci pose des problèmes.

Ensuite, s'il vous plait. En fait, ce que nous observons, c'est un taux de réussite qui est mauvais pour le suivi. Vous avez différents TLD avec les chiffres. Et donc, en fait, le taux de réussite est très bas en termes des principaux domaines de premier niveau.

Il y a plusieurs problèmes. Plusieurs raisons à ceci. Beaucoup des UI ne

sont pas très simples pour les clients à utiliser. Donc les clients ne comprennent pas également comment s'occuper du DS de manière adéquate. Il est également complexe pour les techniciens de suivre le processus. Il y a eu des problèmes. L'algorithme 13 n'était pas compatible avec l'interface des bureaux d'enregistrement et des opérateurs de registres. Il y a également un problème parce que les clients avaient peur que leur zone ne se casse.

Ce que nous avons maintenant, ce que nous faisons maintenant, c'est que nous utilisons le CDS CDNSKEY pour toutes les zones activées. Nous pensons que ceci facilitera les choses pour les clients. Donc, les clients doivent simplement activer le DNSSEC sur le bon portail et donc nous, nous nous occupons du CDS CDNSKEY des bureaux d'enregistrement. Et les opérateurs de registres parents n'ont ensuite pas à s'inquiéter d'autres détails. Donc tout est automatisé.

Ensuite, donc comme je l'avais dit, dès que les clients activent le DNSSEC, les CDS CDNSKEY sont publiés. Donc le parent scanne régulièrement la zone. Nous avons également vérification et notification pour le client, qui peut être ajoutée avec une période d'attente de 24 heures suivant ce que décide le TLD. Et ensuite on effectue les changements du DS. Il faut également faire un scanning régulier de manière à ce que ces choses soient identifiées rapidement.

Ensuite. Donc voilà, je viens d'en parler. Ensuite. Actuellement, nous avons quelques TLD, les .ch, .cz, .li, .cr, qui ont la CDNSKEY et qui commencent le DANS. Nous travaillons également avec Gandi, le bureau d'enregistrement qui nous a beaucoup aidés et nous allons

également communiquer avec d'autres bureaux d'enregistrement sur cette question.

Diapositive suivante. Alors que demandons-nous. Tous les opérateurs de DNS devront le faire par défaut. Nous allons également mettre le DNSSEC par défaut donc les clients qui utilisent Cloudfare devront l'avoir. Et nous allons également utiliser un logiciel open-source. Donc voilà, c'est tout ce que j'avais à vous dire. Merci.

JACQUES LATOUR : Merci beaucoup. Ensuite, nous avons Ondre Filip, de CZNIC, qui va nous parler de la gestion de clés automatisée.

ONDRE J FILIP : Bonjour. Je suis Ondre Filip de CZNIC. J'aimerais vous parler de comment nous avons géré cette question. Diapo suivante, s'il vous plait.

Je pense qu'on sait tous qu'on a un pourcentage de domaines signés DNSSEC, mais nous avons compris que nous pouvions aller un peu plus loin, non pas au niveau des utilisateurs individuels, mais en permettant certaines configurations. Nous avons signé plus de 20 cas au niveau des domaines avec des DS publiés.

Nous savons qu'il peut y avoir certains problèmes et nous avons identifié, donc, certains problèmes. Même si nous essayons d'éduquer tous les bureaux d'enregistrement, parfois leur service n'est pas optimal. Et c'est pour ça que nous essayons d'aider donc à cette

signature de domaine.

Et même si vous êtes des fournisseurs de services, parfois ces services ne sont pas disponibles. Et donc, pour ce qui est des fournisseurs DNS qui n'ont pas de bureau d'enregistrement et n'ont pas de relations avec le registre, certains d'entre vous, vous vous souvenez peut-être de l'époque où l'on mettait donc le registre, on le soumettait à la zone parente et c'était tout.

Donc nous devons changer de choses. La première, c'est la mise en place du DNS Knot. Donc ce Knot DNS établit le DNS de manière automatisée et signe périodiquement les zones, mais peut également publier les clés. Donc périodiquement, il vérifie l'existence de l'enregistrement DANS. Et donc, si ces DS sont là, le roulement de la clé se fait. Et l'on fait le roulement de l'algorithme également. Il faut configurer soit les serveurs faisant autorité soit un ensemble de clés pour compléter la chaine de confiance.

D'autres caractéristiques, cela supporte la CSK, la clé partagée. Mais on peut également avoir des clés individuelles pour chaque domaine. Et comme j'ai dit avant, on peut faire le roulement d'algorithmes.

Si vous voulez retirer la clé à travers une CDNSKEY vide, il faut le faire de manière manuelle. Et on est à la version 2.6 de notre DNS.

Diapo suivante s'il vous plait. L'autre partie de la chaine, c'est le registre. Avant de commencer la mise en œuvre, on a ouvert le débat avec les bureaux d'enregistrement pour voir quelles étaient les options disponibles. Même si on ne va pas les mettre en place toute, il

y en a qui seront mises en place au niveau du bureau d'enregistrement, d'autres au niveau des registres. Et sans surprise, ils ont décidé que c'est à nous de mettre en œuvre cela. Nous avons dit que nous allions vérifier et vérifier les CDS CDNSKEY dans tous les domaines. Nous avons utilisé l'option d'extraire.

Excusez-moi, je vais un peu vite. Je n'ai pas synchronisé les diapos. Voilà, c'est la mise en œuvre par rapport au bureau d'enregistrement. Diapo suivante.

Que faisons-nous ? Nous scannons, tous les jours, tous les domaines dans le fichier de zone. Ça nous prend trois heures. Nous essayons de trouver les enregistrements CDNSKEY. Il y a trois catégories de domaine dans pour cette clé.

Ensuite nous scannons les domaines pendant sept jours. Et s'il n'y a pas de changement au niveau de l'enregistrement CDNSKEY nous considérons qu'il est correct. Ensuite, on a beaucoup de domaines Bootstrap. Et on vérifie les enregistrements DS dans ces zones. Ensuite, il y a certains domaines qui ont des enregistrements DS qui sont déjà faits par les bureaux d'enregistrement de manière manuelle, donc si l'information est complète et si toutes les vérifications sont bonnes, alors on passe automatiquement à la nouvelle clé et on supprime l'ancienne.

Voilà certaines statistiques pour ce qui est des noms de domaine signés. Les chiffres ne sont pas très hauts. 2 %, mais ça évolue. 1700, comparés à plus de 7000.

Diapo suivante. Pour ce qui est de FRED, le système d'enregistrement à source ouverte, nous ne l'utilisons pas, mais il est utilisé par d'autres pays. Bonne nouvelle. Il y a des pays qui ont essayé de suivre notre chemin et de mettre en place ce que nous avons mis ; c'est le cas du Costa Rica qui a mis en œuvre ce système automatisé de gestion de clés.

Diapo suivante. Quels sont les plans pour l'avenir ? Nous essayons de peaufiner le système. Nous devons ajouter plus d'instances de scanning. Nous essayons de voir comment informer les titulaires de noms de domaine, parce que tout ce qu'on leur envoie, c'est un peu confus pour eux. Alors il faut faire quelque chose par rapport à cela.

Ensuite, nous considérons la mise en œuvre d'un modèle de type Push, pousser, pour les Knot DNS et pour FRED. Il faut attendre pour RFC, mais je ne sais pas pour quand ce sera fait.

Ensuite pour les fournisseurs DNS, nous envisageons Cloudflare. Et un point important, il y a eu une présentation intéressante lors de la dernière réunion de RIPE d'une personne de la République tchèque. Il parlait du DNS inverse. Et je pense que c'est intéressant aussi, parce que ce serait intéressant non pas pour traduire des noms dans des numéros, mais l'inverse aussi. Donc ce serait intéressant d'explorer cette piste du DNS inverse. On pourrait en parler peut-être la prochaine fois.

Prochaine diapo- et c'est tout de ma part. Merci beaucoup.

JACQUES LATOUR : Merci, Ondre. Notre prochain un intervenant, c'est Michale Hausding, de Switch, qui va parler de l'automatisation du DNSSEC avec CDS.

MICHALE HAUSDING : Merci beaucoup. Nous avons donc mis en place une initiative il y a deux semaines. Nous avons les premiers domaines qui sont mis dans la zone .ch. Nous avons eu un impact très utile. Donc je vais vous parler notamment sur quelles ont été nos motivations et quelle est notre expérience.

Tout d'abord l'adoption du DNSSEC en Suisse augmente, mais je pense qu'on doit faire davantage pour la promouvoir. Certains des bureaux d'enregistrement n'ont pas utilisé DNSSEC, et pourquoi ? Tout d'abord, parce qu'il y a un système de registres qui n'est pas capable d'automatiser DNSSEC. Et donc cela requiert beaucoup de travail au niveau de la mise en œuvre. Et deuxièmement, parce qu'ils ont peur des roulements de clé.

Alors si on regarde la manière dont on travaillait avant, on a les bureaux d'enregistrement qui créent des clés dans leur zone. Cette clé, après, elle était poussée vers le registre. Pour cela, le bureau d'enregistrement doit prendre la clé du serveur ; il doit la télécharger pour le registre, parfois à travers une interface ou par e-mail, pour que cette clé arrive au registre à travers le EPP. Certains bureaux d'enregistrement par exemple ne peuvent le faire que via e-mail pendant les jours de la semaine. Et donc parfois, il faut attendre donc les jours de la semaine pour recevoir cette clé. Être lundi au bureau

pour avoir cette clé. Après avoir activé CDS, les choses se simplifient.

Il faut allumer la signature des noms de votre serveur et les registres peuvent obtenir directement de ce serveur la clé. En théorie, ils peuvent obtenir la clé et la publier. Il y a des décisions à prendre par rapport à ce processus.

Si on regarde pourquoi nous faisons cela, parce que cela rend l'automatisation beaucoup plus facile : à partir du moment où vous publiez la clé, le registre obtenir. Et il n'y a pas d'autre système en place. Le roulement, si vous choisissez de faire un roulement, vous ne vous inquiétez pas, parce que le roulement se fait de manière automatique. Et avec CDS, il y a un mécanisme pour mettre à jour la zone et la zone parente pour le roulement.

Nous voulons également montrer que DNSSEC n'est pas si compliqué que ça au niveau de l'utilisation. Si vous regardez, cela ne vient pas d'un serveur faisant autorité, c'est juste une ligne qu'il faut ajouter au niveau de la configuration. Et la bonne nouvelle avec Knot, c'est qu'il y a beaucoup de choses qui sont par défaut, ce qui permet la publication de la CDS de manière automatique. Donc c'est juste une ligne que l'on ajoute pour activer la signature DNSSEC, et si le registre peut si possible obtenir la clé CDS, c'est fait. Il n'y a que deux lignes de configuration qu'il faut changer pour cela.

Nous suivons des normes. Pour le moment, nous n'avons pas eu problème. La question est toujours de savoir comment nous le mettons en place. Cela n'est pas dans le RFC.

Nous avons deux cas de figure. Un cas où la zone est déjà validée et c'est assez facile ; nous validons ou nous vous obtenons le CDS directement de la zone fille, nous validons via DNSSEC et si la CDS ne change pas pendant trois jours, nous mettons à jour les paramètres. Ce qui est un peu plus compliqué ou ce qui rend les choses un peu moins simples et qui prend un peu plus de temps, c'est savoir comment nous faisons pour le Bootstrap si la zone n'est pas validée.

Si la zone n'a pas de DS dans la zone parente et il n'y a pas de confiance initiale comme point de départ, alors nous devons construire cette confiance initiale. Nous devons avoir une certaine confiance, au moins dans les serveurs de noms faisant autorité. Donc nous disons OK. Nous allons vérifier toutes les instances du serveur faisant autorité et, si elles nous donnent toutes la même adresse pour la même requête, alors peut-être qu'on peut lui faire confiance.

Le deuxième élément, c'est éviter le détournement, le spoofing. Il n'y a pas moyen de changer, d'usurper les réponses. On analyse cela pendant trois jours. Nous croyons qu'on pourrait pirater quand même par BHP tous les noms du serveur. On les vérifie donc pendant trois jours pour nous assurer qu'il n'y a pas de problème. Donc ce sont des requêtes qui viennent de différents points. Et donc ce serait très difficile de pouvoir pirater tout cela. Et si nous voyons qu'il y a une réponse qui est cohérente pendant trois jours et que la CDS ne change pas pendant trois jours avec des requêtes qui viennent de différents points, alors à ce moment-là, on la place dans la zone parente.

Il y a eu une question ce matin, que faisons-nous si la validation

DNSSEC ne marche pas ? Si nous utilisons le modèle extraire, le modèle Pull, nous validons avec la CDS que nous avons obtenue. Et sinon, on l'obtient de la zone parente. On ne peut pas mettre en panne le DNSSEC en publiant une CDS erronée. On peut la casser sur EPP si on met une clé erronée.

Il y a certains algorithmes qui sont inclus. Nous ne communiquons pas les e-mails. Nous parlons avec CZNIC. Usuellement, ils envoient un e-mail. Si on envoie un e-mail au contact technique, pour la plupart du temps, ça ne marche pas. La personne n'est pas très technique. Et c'est pour ça que nous avons choisi une approche différente.

Nous avons dit d'accord, essayons de donner à chaque contact technique la possibilité de voir quel est l'état du processus de publication de la CDS. Et donc nous avons mis en place ce qu'on appelle la vérification de statut de la CDS. Très bien. Nous pouvons aller à nic.ch/cds. Sur ces URL, vous pouvez trouver donc le statut des CDS et nous donnons la date à laquelle nous avons mis la CDS dans la zone parente.

Pour ce qui est du Bootstrap, voilà, maintenant on voit que ça fonctionne. Pour ce qui est du roulement, l'un des bureaux d'enregistrement l'a autorisé il y a deux jours. Actuellement nous sommes à la période où cette configuration est disponible et donc les bureaux d'enregistrement doivent le faire. L'un d'entre eux l'a fait. Voilà le résultat. Nous avons envoyé des requêtes trois fois aujourd'hui, et demain, nous allons donc la mettre dans la zone CDS. Voilà. C'est l'un des premiers noms de domaine que nous avons via

CDS, via le système CDS.

Les chiffres, c'est plus ou moins les mêmes. On a 2 % des DNSSEC signés. Nous avons 15 000 signatures de domaine et 900 enregistrements CDS. Pour ce qui des bureaux d'enregistrement, nous avons Cloudflare, Google Domains, Internet hosting qui sont les trois premiers. En janvier, nous allons mettre les enregistrements DNS dans la zone .ch. Merci.

JACQUES LATOUR : Merci beaucoup. Ensuite, donc nous avons Richard de GoDaddy qui va nous parler de ce que fait GoDaddy et de son soutien, de sa compatibilité totale.

RICHARD MERDINGER : Alors, tout d'abord, j'aimerais remercier Steve Crocker parce qu'il m'a invité en tant que bureau d'enregistrement. GoDaddy est un grand bureau d'enregistrement, mais nous sommes également le plus grand fournisseur de DNS.

Nous avons une diapositive qui va arriver j'espère.

Alors, lorsqu'on parle à GoDaddy, on pense à un bureau d'enregistrement pas à un fournisseur de DNS. Nous avons activé le DNSSEC depuis un certain nombre d'années. Nous avons parlé à Steve pour mettre ceci en place et nous en sommes au point où, étant donné que nous sommes un bureau d'enregistrement avec un lien aux opérateurs pour la zone DNS que nous gérons, nous avons en fait un

roulement automatique de clé en un clic dans notre écosystème.

Donc nous avons été assez focalisés sur notre écosystème. Et donc maintenant, nous souhaitons aider l'écosystème plus large. Parce que GoDaddy, nous avons beaucoup de services ; nous avons également un service qui est bureau d'enregistrement, nous avons un service qui est DNS. Cloudfare même chose ; c'est bureau d'enregistrement et DNS.

Donc d'une manière générale, nous sommes d'accord avec l'idée de la CDNSKEY, et la mise à jour directe à partir du service DNS vers le bureau d'enregistrement. Nous avons une relation avec l'opérateur de registres en termes de changement du paradigme des services que nous fournissons pour le titulaire de noms de domaine. Donc en ce qui concerne la mise en marche ou l'arrêt du DNSSEC, nous croyons réellement que ceci doit passer par le bureau d'enregistrement pour le mettre en place, avec des mises à jour par la suite en continu.

Nous savons tous avec le CDNS que ceci peut se passer de manière très fluide, mais il faut une mise en œuvre au niveau du registre. Et suivant la taille de la racine de la zone, il peut y des problèmes où le scanning prend longtemps et il y a des couts d'infrastructure, etc. Donc, il n'y a pas une seule solution à notre avis ; il doit y avoir un ensemble de solutions qui, pour certaines, voudront dire un investissement, une mise en œuvre. Notre technicien devait être aujourd'hui ici. Mais il a dû partir hier. Donc nous avons fait un développement à l'interne avec un protocole public qu'on appelle Domain Connect. Donc Domain Connect, c'est en fait un paradigme

qui permet d'activer les FSI, les hébergements, les fournisseurs d'hébergement, n'importe quels, en fait, services ou fournisseurs, avec un service qui permet d'activer. Et donc, si par exemple quelqu'un va sur Wix ou Weebly, ou donc un site Web, on peut mettre le nom de domaine, le système Domain Connect identifie la bonne configuration de DNS, voit où est le fournisseur d'avitaillement, où est le soutien de DNS. Il y a un système en place qui permet à Cludfare ou au fournisseur de services d'appliquer un modèle à la zone qui ne possède pas vers le fournisseur de DNS. Donc en fait, ça découpe les services. Ça divise les services plutôt du fournisseur de DNS. On a l'impression qu'il n'y a pas d'intermédiaire. Donc, la mise en œuvre est sans problème.

Nous avons parlé d'augmenter le service de Domain Connect donc de l'augmenter, de l'élargir de manière à ce que les enregistrements DNS puissent également être mis à jour, de manière à ce que le bureau d'enregistrement considère d'être séparé. Donc le service du bureau d'enregistrement serait souscrit à DNS Connect, et le fournisseur pourrait faire une mise à jour de son enregistrement DS. Et donc l'idée ce serait d'utiliser EPP. Le bureau d'enregistrement donc ne mettrait pas en œuvre tout le mécanisme.

D'une manière générale, nous sommes pour faire ce qui a été présenté, mais nous souhaitons qu'on fasse attention par rapport au changement de paradigme par rapport à l'extension de DNS. Mais il y a eu une exception pour fonctionner dans le DNSSEC. Nous ne souhaitons pas empêcher les mises à jour continues qui devraient avoir lieu.

Donc voilà tout ce que j'avais à dire. Je n'avais qu'une diapositive.

JACQUES LATOUR : Merci. Je n'ai que 100 questions là-dessus ! Première question. Je vais d'abord poser la mienne. Mais première question pour Vicky.

Vous avez parlé de Cloudfare et du fait que vous publiez le CDSKEY 0, plutôt que de n'avoir que CDS et CDNSKEY, c'est ça ?

VICKY SHRESTHA : Non. Cloudfare publie CDS et CDNSKEY pour toutes les zones activées DNSSEC. Nous avons ajouté le CDS 0, et le CDNSKEY 0 si le client choisit de désactiver sur son portail.

JACQUES LATOUR : Donc n'est pas un nouveau type d'enregistrement ?

VICKY SHRESTHA : C'est juste, oui, c'est juste une option. Si par exemple le client désactive le DNSSEC, s'il souhaite procéder de cette manière.

JACQUES LATOUR : D'autres questions ?

PETER KOSH : Je m'appelle Peter Kosh. Je suis sceptique en termes de motivation,

de soutien des CDS et CDNSKEY. Michale disait qu'une des raisons c'était que le roulement est compliqué, et donc pourquoi le faire. Si je me souviens bien des motivations pour l'idée du roulement de clé, c'était de former le personnel en cas d'urgence de roulement, de manière à ce que les gens soient prêts à le faire, ce roulement. Maintenant, ce qui se passe, c'est qu'on se rend compte que, finalement, aller faire de l'exercice, c'est complexe. Donc on emploie des étudiants, à savoir l'automatisation pour aller faire de la gymnastique pour nous. Et donc un petit peu étrange cette histoire d'automatisation. Parce qu'en fait cette urgence de roulement urgent nécessite beaucoup de travail. Donc le transfert pour les opérateurs de registre, il faut encore interagir avec les registres et les bureaux d'enregistrement. Maintenant qu'est-ce qui se passe avec le modèle CDS et CDNSKEY ? Comment est-ce que ça marche ?

MICHALE HAUSDING : Première chose, le roulement de clé. Le roulement de clé pour les domaines de deuxième niveau est complètement différent que le-

INTERPRÈTE : Désolée, l'interprète a des problèmes de son.

MICHALE HAUSDING : Donc le roulement de clé pour le deuxième niveau est différent. Donc la plupart des utilisateurs peuvent le mettre, mais ne comprennent pas comment ça fonctionne. Donc, les former, c'est vraiment quelque

chose qui doit rester auprès du serveur de DNS. Alors ça, c'est pour les roulements de clé. Si vous voulez faire un roulement de clé. Mais il n'y a pas de formation du côté du titulaire de noms de domaine par rapport au roulement de TLD.

Alors c'était la deuxième question, quoi déjà ? Le roulement urgent et les changements d'opérateurs de DNS. Oui. Donc, imaginez-vous en cas d'urgence. Il y a deux possibilités. Un, vous avez le roulement en urgence avec le CDS, il faut le faire sur le serveur de DNS. Donc, dès qu'on roule la clé dans le serveur de DNS, CDS s'en rend compte et c'est parti. Autre possibilité, se rendre sur place en cas d'urgence. Ce n'est pas ce que nous recommandons, mais c'est pour ça que nous avons l'algorithme 0 qui permet d'indiquer à la zone parente que vous souhaitez vous rendre sur place. Donc ça, c'est une autre possibilité. Voilà pour le CDS. Nous ne scannons la zone qu'une fois par jour, donc vous avez un retard de jusqu'à un jour avant de savoir qu'il faut faire un roulement en urgence ou se rendre sur place.

Mais on a également la possibilité pour le CH de pousser une nouvelle clé ou de l'éliminer de la zone. Mais il faut un certain temps. Il faut le savoir.

JACQUES LATOUR : Steve, vous avez une question ?

STEVE CROCKER : Oui merci, Jacques. Trois choses. Je souhaite répondre directement à

la question très intéressante de Peter. Merci d'ailleurs.

Si je comprends bien, le roulement est une bonne pratique ; il doit être fait régulièrement, pas uniquement en cas d'urgence. Les algorithmes, les clés, n'ont pas un délai de vie normale. Et même si on pouvait dire qu'on n'a pas besoin de rouler la clé nécessairement, pendant assez longtemps, le système ne sera pas durable à long terme. C'est une mauvaise idée. Donc le roulement de clé c'est surtout en cas d'urgence. Donc cette idée que la clé est uniquement en cas d'urgence, à mon avis, n'est pas la bonne approche. Ça doit être fait de manière régulière.

En termes de changement d'opérateur de DNS, donc c'est une fonction qui est importante à avoir. Récemment, il y a eu une présentation de [Schuman Hawk] qui parlait non seulement du passage d'un opérateur à un autre, mais également d'avoir différents opérateurs indépendants qui sont au service du même client. Et c'est la version. Donc, ce passage d'un opérateur à un autre, donc en fait vous n'éliminez pas le service du premier opérateur, à mon avis, c'est une solution complète ; une excellente solution en cas de changement d'opérateur.

Alors je reviens maintenant à la question que j'allais poser. Qu'est-ce qu'il faut faire encore ? Il y a beaucoup de présentations ici qui se focalisent sur la solution CDS CDNSKEY et le fait que les registres tirent ou extraient l'enregistrement. Donc toutes les présentations sont toutes du point de vue ccTLD et non pas du point de vue gTLD. Quelle est votre estimation ? Que va-t-il falloir faire pour amener ce type de

solution dans l'espace des parties contractantes de l'ICANN.

Et vous avez également l'autre approche avec un modèle twist, un autre modèle d'interface approprié. Et donc j'aimerais répéter ce que j'avais dit au début. Moi je n'ai pas d'intérêt dans quoi que ce soit. Simplement je souhaite que ça fonctionne. Et ma préoccupation, c'est avoir quelque chose d'installé sur la moitié des parties avec donc cette moitié qui dit bon voilà ce qu'on fait, et puis vous avez l'autre moitié qui dit non, ça ne nous intéresse pas. Moi je ne veux pas me retrouver coincé entre ces deux.

JACQUES LATOUR : Merci, Steve. Alors, il y a beaucoup de questions à mon avis, mais une des plus grosses questions, c'est le processus de Bootstrap. Comment est-ce qu'on obtient le DS dans la zone ? Comment est-ce qu'on met le DS dans la zone ?

Donc lorsqu'on a commencé cette discussion, d'une manière générale, les gens hésitaient à prendre le DS ou le CDS. Et maintenant, on y arrive petit à petit avec les ccTLD. Alors pour les gTLD, la définition de la politique par rapport à ça est très large, très faible. Donc devons-nous créer un texte plus approprié qui définit l'acceptation du DS par les gTLD. Quel est le processus pour que le DS s'applique aux registres ? Quelles sont les options qu'on n'accepte pas ? On peut savoir quels sont les protocoles à mettre en place, parce que actuellement on ne sait pas où on en est. Donc il est un petit peu complexe d'avoir des processus si on ne sait pas où on en est.

Petit exemple, si vous créez un domaine .ca et que la fille est signée tout de suite. Vous avez un enregistrement DS c'est un nouveau domaine, je viens de le créer dans mon registre. Si je l'extrais, que je prends le CDS et que j'ajoute le DS tout de suite, ça, va à l'encontre d'une réaction qui serait la réaction immédiate. C'est la deuxième fois qu'on a un panel un petit peu politique là-dessus et on avance. Mais pas assez rapidement

RICHARD MERDINGER : Oui, dans le contexte, si j'ai bien compris, le registre lance l'extension de DNSSEC. C'est ça ? Donc le bureau d'enregistrement ne crée pas le registre et le registre fait partie de cette transaction à multivolets pour le DNSSEC et donc ceci rentre toujours dans le paradigme. C'est la politique, mais c'est le bureau d'enregistrement qui crée. Donc là, ce n'est pas ça le problème. Mais vous avez créé un domaine, n'est-ce pas ? Et vous créez toujours un domaine.

Oui, mais si on crée un domaine et que la politique de registre est de ne pas utiliser le DNSSEC, par conséquent, le DNSSEC doit être lancé par le bureau d'enregistrement. Donc on a une transaction à multivolets qui mène à un DNSSEC lancé par le bureau d'enregistrement.

Autre scénario. Il y a deux transactions, une qui crée et une autre qui étend DNSSEC. Je ne sais pas si je suis trop compliqué, mais en fait, c'est comme ça que ça marche à l'ICANN.

JACQUES LATOUR : Je pense un petit instant. Si vous créez un domaine, par exemple .com- je vais finir. Si vous créez un domaine .com et donc GoDaddy peut prendre le DS et le mettre dans la zone. C'est ça ?

RICHARD MERDINGER : Oui. Nous faisons cela pour notre zone DNSSEC. Cela fait partie du fait d'être partie de l'écosystème.

JACQUES LATOUR : Paul.

PAUL WOUTERS : Je suis l'un des deux auteurs du RFC. La raison pour laquelle nous avons voté, c'est parce qu'il y avait une demande de la part des opérateurs de registres de l'avoir, parce que très souvent, un client va changer d'hébergeur DNS, mais pas forcément de bureau d'enregistrement. Et l'utilisateur titulaire de domaine ne connait pas ces détails techniques, et il change tout simplement de fournisseur DNS. Il ne comprend même pas ce que c'est DNSSEC. Donc si on passe d'un hébergeur DNS qui n'a pas la capacité d'avoir DNSSEC, il faut informer le titulaire de nom. Même si le titulaire ne sait pas, l'hébergeur le sait, et c'est pour ça qu'on a travaillé par rapport à cela.

JACQUES LATOUR : Merci.

RICHARD MERDINGER : Je peux répondre ? Il y a certains éléments- pardon, excusez-moi, j'ai tapé le micro. Les lignes ne sont pas très nettes ici.

Il y a certains éléments où la base de données de registres a des attributs du nom de domaine. Certains de ses attributs vivent aussi dans la zone racine. Alors je vois que les noms de serveur, il y a une sélection de fournisseurs de serveurs de noms, et les enregistrements DNS sont des composantes de configuration de domaine, même si l'on fait partie de l'écosystème en ce qui concerne le DNS. Excusez-moi, j'ai perdu le fil.

JACQUES LATOUR : Steve avait une question.

STEVE CROCKER : Merci. Ma question est d'essayer de savoir — c'est pour Rich — si les registres récupèrent l'information. L'un des commentaires que j'entends, du point de vue de la politique, c'est que le bureau d'enregistrement doit avoir des informations claires par rapport à la zone. Et c'est l'une des raisons pour lesquelles il ne devrait pas y avoir un chemin. Parce que le bureau d'enregistrement doit avoir toutes les informations.

Comment vous pensez que la nouvelle information DS va de l'enfant au parent si elle ne va pas du client vers vous.

RICHARD MERDINGER : Merci. Pour le paradigme original, je dirais que c'est aussi simple que les scans des registres mettent à jour l'information ; cela est notifié pour que les autres mettent à jour leurs systèmes. Il y a des moyens de faire en sorte que l'on puisse mettre à jour donc ces informations. Nous essayons de mettre en synchronisation tous les systèmes.

Désolé. Il y a beaucoup d'interférences.

RICK WILHELM : Rick Wilhelm, VeriSign. Avant, nous avons parlé de l'enregistrement pendant le processus de création. Dans mon expérience, il y a un bureau d'enregistrement précédent et un opérateur de registre actuel, la plupart du temps, le titulaire intervient dans le chemin d'enregistrement.

Quand j'étais un bureau d'enregistrement, je ne voulais pas retarder les processus. Je ne sais pas ce que vous avez fait, Richard, mais la plupart du temps, il y a une création et donc l'addition du DS est un processus qui a lieu après la création.

RICHARD MERDINGER : Très brièvement, je vais dire qu'il y a beaucoup de domaines qui sont achetés et qui n'ont pas par défaut DNSSEC.

JACQUES LATOUR : C'est un ou deux ? Deux c'est une réponse à ce qui existe.

INTERVENANT NON IDENTIFIÉ : Il y a une extension EPP où le registre se connecte avec le bureau d'enregistrement pour obtenir de nouvelles informations du DNS pour pouvoir mettre à jour leur enregistrement.

JACQUES LATOUR : Patrick.

PATRICK FALLSTRÖM : Je pense que nous commençons à allumer ou éteindre la fonction DNSSEC, mais il y a la question de savoir qui a la responsabilité pour la zone pour que la zone travaille. Et c'est un contrat contractuel entre le bureau d'enregistrement et le titulaire de nom. Et donc tout ce qui se passe pour allumer et éteindre DNSSEC, cette opération, comme je l'ai dit à l'IETF très souvent, c'est quelque chose qui relève de la responsabilité des bureaux d'enregistrement.

Ce n'était pas moi, ce bruit.

Pour ce qui est de la mise à jour des enregistrements DS, quand le DNSSEC fonctionne, c'est une autre chose.

RICHARD MERDINGER : Je n'ai pas compris si c'est la une ou la deux. Excusez-moi. Mais pour Patrick, la possibilité de faire fonctionner DNSSEC. Excusez-moi, je ne peux pas parler en ce moment.

JACQUES LATOUR : Y a-t-il d'autres questions ? Je pense que nous pouvons continuer à en parler pendant des jours. Mais bon, je vais remercier les panélistes pour cette séance.

RUSS MUNDY : Très bien. Merci beaucoup à tous les panélistes. Nous apprécions vos contributions. Notre prochaine séance, notre prochain panel portera sur le sujet favori de nous tous, c'est le roulement de la KSK. Nous avons Wes Hardaker et Matt Larson, Wes Hardaker va parler en premier. Quand vous serez prêt, Wes, je vous donne la parole.

WES HARDAKER : Allez-y. Je sais qu'on a un peu de retard. Je travaille à l'institut de recherche de l'Université de Californie du Sud. Je vais vous parler de roulement de clé dans une des instances de la racine. C'est là où ma perspective est passée d'inquiétude à un certain calme à la fin.

Alors voilà un petit peu un aperçu. Je vais commencer avec mon état paranoïaque et puis on va voir la réalité, à quoi elle ressemble.

D'abord ma paranoïa, c'était de savoir ce qui se passe si le monde reste déconnecté d'Internet. C'était un état un petit peu paranoïaque dans lequel je me mettais. Que se passerait si les résolveurs deviennent fous. Et cela, ici, vous voyez un schéma qui était l'une de mes plus grandes craintes, où l'on voit un énorme trafic en rouge. Vous voyez les opérateurs de racine ont vécu ça à un moment donné.

Et donc, cette paranoïa m'a dit conduit à analyser beaucoup de

données et j'ai analysé des mauvaises configurations du logiciel VPN. On a corrigé certains problèmes avant le roulement de la clé. Et maintenant, je vais vous parler de mon incapacité à trouver beaucoup plus que ça.

Alors qui était en problème ? Qui pouvait être impacté ? Et c'est vraiment la question que nous nous posions tous, voir qui pourrait être impacté par cela. Il y avait deux choses ; d'un côté, il fallait savoir quelle était la clé qui devait être configurée, donc il y avait le RFC 8045, et ensuite, la signalisation KSK. Mais ce ne sont pas des documents complets. Donc je pense que si nous allons revoir les choses, il faut voir comment. Maintenant, on a beaucoup plus d'informations par rapport aux mesures, mais on n'en avait pas avant.

Ensuite, il faut savoir si les serveurs sont en train de valider, si c'est possible. Si le résolveur valide, il fallait savoir si on pouvait avoir ça à partir du trafic. Voilà un petit peu de contexte par rapport au comportement des résolveurs et comment fonctionne la résolution par rapport au résolveur de validation.

Tout d'abord, le réseau dit à la racine, est-ce que vous avez www.exemple.com ? Et vous savez comment ça fonctionne. Ensuite la racine lui répond avec le record Glue où on inclut l'enregistrement DS et la signature de ces registres. Très souvent, le résolveur renvoie une requête au DS à la racine. Ce n'est pas obligatoire, mais cela est fait quand même fréquemment. On ne sait pas très bien quels sont les résolveurs qui le font, et ceux qui ne le font pas. Mais par exemple, on sait que BIND le fait pour vérifier les données dans une section

supplémentaire.

Voilà. Cela m'a amené à l'hypothèse de dire que 50 % des requêtes devraient être pour des enregistrements DS et l'autre 50 % pour des questions d'origine. Alors je pense que la question est de savoir y a-t-il d'autres questions que l'on doit se poser ? Ce sont les seules requêtes que l'on devrait envoyer.

Alors première étape, il faut retirer toutes les requêtes qui ne sont pas les requêtes pour ce qu'on vient de voir. Et vous voyez donc en orange les différentes requêtes. Vous voyez ces données qui ne servent à rien, qui sont en orange. Et je pense que voilà, c'est important de voir que Chrome envoie beaucoup de chaines de manière randomisée.

Ensuite, on a vu qu'il y avait des requêtes pour une étiquette simple comme .com, etc. Voilà le résultat de mon enquête, j'avais raison.

Si on voit quelles sont les requêtes envoyées, les serveurs racine 50 % des requêtes, ce sont des requêtes DS, donc l'axe horizontal, c'est le pourcentage et l'axe vertical c'est le nombre d'hôtes qui envoient ce pourcentage. Vous voyez deux courbes géantes ; 50 % d'un côté qui selon mon hypothèse est vrai, et plus l'hôte envoie des requêtes plus on se rapproche du 50 %. Et on voit les données de la racine juste avant le roulement de la clé. À gauche, je ne suis pas très sûr pourquoi les gens enverraient 10 %, mais en supposant que mon hypothèse est correcte, j'ai décidé d'aller voir toutes les informations disponibles.

On va donc se concentrer sur les requêtes envoyées. Plus de 25 %, ce sont des requêtes DS. Tout cela correspond à septembre 25, c'est-à-

dire avant le roulement.

Question suivante. Lesquels de ces valideurs étaient en train d'envoyer seulement des signaux de validation pour la KSK 2010, seulement ? Et ce sont les requêtes envoyées par Chrome, notamment. Il y a 45 806 résolveurs dans ce groupe. Le nombre total de résolveurs envoyant la KSK 2016 était 420. Heureusement, il y avait beaucoup qui n'avait pas encore la nouvelle clé.

Est-ce que vous voulez savoir combien envoyaient l'ancienne clé ? 12, ce qui représente une réduction de 18 par rapport au mois précédent. Donc ce sont des résolveurs de validation. Seulement 12 de ces résolveurs envoyaient l'ancienne clé. Et donc cette différence m'a fait sentir beaucoup mieux. Et donc j'étais un peu plus préparé au roulement qui allait être fait la semaine suivante. Je me sentais un peu plus à l'aise.

Donc question suivante. Quels sont les enregistrements DS qui étaient envoyés ? Quelles étaient les requêtes ? Les résolveurs normalement envoient uniquement des requêtes DS pour Com, pour un TLD ; jamais pour exemple.com. Donc le résolveur est raisonnable, surtout lorsque je suis rentré dans le détail de ces 12 résolveurs. Beaucoup d'entre eux, c'était des requêtes ne servaient à rien.

Donc dans la vie réelle, comment ça se passe. Je vais vous montrer des diagrammes de nos opérations, peu importe quelles sont les lignes. Mais là, cela vous montre le trafic vers les serveurs racine. Donc c'est assez juste avant le roulement. Si vous regardez avec attention à

droite, vous verrez que toutes les lignes justement du roulement remontent. Et donc là on a eu peur. Les gens se disent, mon Dieu, le ciel va nous tomber sur la tête. Et donc là, vous voyez la petite bosse quelques heures plus tard. Tout est revenu à la normale et nous avons une ligne complètement plate après. Donc la ligne plate, ça veut dire que tout est resté en vie. Ce n'est pas comme sur un électrocardiogramme. Donc dans la vie réelle, vous voyez, les choses s'améliorent.

Deux choses importantes. Donc mise à jour des logiciels et des configurations, ça va. Ça s'améliore. Les choses se sont bien passées. Je pense que l'année supplémentaire que nous avons eue représente une excellente décision par Matt et par son équipe, parce qu'on n'était pas prêt, il y a un an. Cela nous a donné suffisamment de temps pour attendre que les choses s'améliorent.

Dernière chose, les résolveurs sont étranges. On pense les comprendre. Mais à chaque fois qu'on rentre dans le détail pour voir ce qu'ils font, finalement on ne comprend pas. Donc il y a un caucus qui est en train de mettre en place une étude de résolveur avec RSSAC et donc nous attendons avec impatience de voir quelles seront les données. Parce que pour ce qui est de Circle K, il y a des choses qui sont étranges. Vous savez, j'ai pris ça. Ça, c'est une citation. Et donc il faut mieux comprendre les résolveurs parce que, à l'avenir, que ce soit le roulement ou autre chose, il nous faut absolument mieux comprendre ce qui se passe.

JACQUES LATOUR : Merci beaucoup, Wes. Nous allons maintenant passer à Matt et nous prendrons vos questions après sa présentation.

MATT LARSON : Matt Larson, vice-président de la recherche dans le bureau technologie, et j'ai été impliqué dans le roulement de la KSK. Alors quel suspense, n'est-ce pas ? Mais sachez que nous avons roulé la clé. Donc ça s'est bien passé. Ça s'est bien passé, dans les temps comme cela avait été prévu. Et j'ai quelques données à vous communiquer.

Ça arrive. Ça arrive. C'est extraordinaire, l'informatique. Alors en attendant, encore une petite chose. Je suis allé voir il y a deux jours les données pour voir le nombre de résolveurs qui avaient été en échec. Donc on était à 10. Donc ça fait deux de moins que les 12, mais ce n'était pas les mêmes en fait. Ça ne fait pas partie du groupe précédent.

Adobe nous énerve. Voilà. C'est bon.

RUSS MUNDY : Nous l'avons dans la salle, mais je pense qu'à distance ils n'ont pas la présentation, mais Matt allez-y.

MATT LARSON : Donc le roulement s'est produit avec la publication d'une zone racine le 11 octobre 2018 à 16 heures UTC. Alors voilà un petit peu ce qui s'est passé en termes d'horaires si ça vous intéresse.

Nous avions trois heures où nous avons passé un peu plus de temps à regarder ce qui se passait dans la zone racine. Donc avant, en général, l'ICANN n'inspecte pas la zone racine avant publication, mais dans ce cas, VeriSign a vraiment regardé ce qui se passait ; l'ICANN aussi. On voulait absolument s'assurer que tout le monde était prêt, d'être sûr que tout se passe bien. Et ensuite, tout s'est passé à l'heure. On l'a lancé d'Amsterdam. Donc VeriSign, ICANN, là-bas, s'en sont chargés.

On voulait être sûr. DNS [org] ne voulait pas être dans l'avion. On s'est dit qu'on va tout faire à Amsterdam. Donc on nous a accueillis ; NL, merci beaucoup.

Et en bas à gauche, vous avez une copie de la zone racine lorsqu'elle a été signée pour la première fois en 2010. Donc on a voulu faire un petit peu un historique. Vous voyez la personne a un petit peu vieilli. Ce n'est pas grave.

Autre chose que nous avons observée, si vous regardez le nombre de requêtes DNS key dans la racine, il y a eu une augmentation. Alors malheureusement, j'avais une petite vidéo, mais elle ne marche pas, donc je suis désolé. Ce n'est pas très logique comme c'est présenté, mais regardez en haut à gauche. Donc vous avez les requêtes DNS key de chaque serveur racine qui donnent des données statistiques à l'ICANN, et en haut, vous avez donc toutes les racines. Tout est cumulé en termes de données. Donc vous voyez un petit peu que l'échelle change malheureusement. Donc il semblerait que c'est la même chose, mais ce n'est pas le cas. Donc 1400 requêtes par seconde, c'est le maximum. Et à droite, vous avez le roulement de la KSK tout à

droite, le 11 octobre. Donc ensuite, vous avez donc 48 heures après le roulement de clé. Et vous avez en haut l'échelle de 2500 à peu près par seconde. Et maintenant, vous avez un maximum de 4000 requêtes par seconde.

Et donc, si on revient en arrière, en jaune vous le voyez à peine, mais vous avez les données d'il y a une semaine. Donc si vous posez la question de savoir si la requête continue à l'éternité, non pas du tout. Parce que ça fait déjà plus d'une semaine, et le jaune et le rouge sont au même niveau. Donc on en est à un plateau.

On a essayé de voir ce qui se passait. On vient de commencer la recherche. Et il y a un excellent travail qui se fait par l'équipe. On s'attendait à avoir davantage de requêtes DNS key sur la base des comportements des résolveurs, parce que lorsqu'il y a un manque de confiance, le résolveur essaye d'avoir des correspondances. Et ça, ce n'est pas possible. Donc il y a des requêtes, des requêtes, des requêtes, et la quantité de requêtes dépend d'un résolveur spécifique.

Donc ce qu'on a décidé de faire, c'est de regarder les comportements des requêtes DNS key avant le roulement. Donc le 10 et le 14 octobre, donc il y a eu 1 million de demandes de DNS key sur les quatre jours, mais nous avons vu 155 000, le 10 et le 14. Et 85 000 résolveurs qui ont envoyé une requête au moins une fois par jour.

Et donc, vous voyez, là. C'est quelque chose qu'on a ; c'est les données par paquets. Donc, regardons ces 155 000 résolveurs qu'on a observé le 10 et le 14 octobre. Sur ce graphique, cela vous explique un petit

peu les choses. Alors je vous montre d'abord l'explication.

Donc l'axe du X, en bas, représente le nombre de requêtes envoyées par le résolveur DNS key, envoyées le 10 octobre, et sur l'axe Y, le nombre envoyé le 14 octobre. Donc chacun des points représente un résolveur. Et donc ce que l'on souhaitait dans la zone verte, donc vous avez le même ordre en magnitude, en ampleur, le 10 et le 14. Donc en fait X et Y sont égaux. Donc chacun des carrés représente à peu près une parité de 10. Donc vous voyez une concentration en bas à gauche. Vous avez les résolveurs qui envoient des petits nombres de requêtes DNS, de 10 à 100. Vous voyez quand vous montez à droite, vous avez un volume de plus en plus élevé. Donc en violet, dans le cercle, vous avez ceux qui ont envoyé beaucoup plus de requêtes le 14 que le 10. Comme vous le voyez potentiellement, vous avez une ampleur supérieure par rapport à donc ces regroupements, donc c'est un, deux, trois de plus, le 14. Par ordre de grandeur.

Donc voilà le type de choses que l'on cherche à analyser. Alors, ceci vous montre le nombre de résolveurs et dans quelle catégorie on les retrouve en termes de grandeur ou de changement.

Donc je reviens ici. Donc là, c'est le résumé de ce que je souhaite vous expliquer.

Pratiquement 96 % des résolveurs sont restés dans cet ordre de grandeur en augmentation ou en baisse pour les requêtes de DNS key. Mais il y en a qui sont allés plus haut. Il y en a qui sont absolument incroyables, qui n'arrêtent pas d'envoyer des requêtes DNS key. C'est

vraiment une grosse augmentation. Et également, il faut bien savoir qu'il y a un nombre plus important, donc 4500, qui envoient moins de requêtes DNS key. Donc on en est à la phase initiale de cette investigation. Donc je ne peux pas vous en dire plus là-dessus. Nous allons continuer de regarder ce qui se passe pour essayer de comprendre. J'espère que ce ne sera pas un mystère qui va rester éternel comme d'autres mystères, comme la radiation sur Internet des choses qu'on ne comprend jamais.

Désolé. Ça n'a pas marché, là. On le voit, mais ce n'est pas très clair. Bon. Tant pis. De toute façon, ça ne me plait pas. Donc c'est très bien.

Donc là, c'est le rapport RFC 8045, donc l'ensemble de données qui a amené à la décision de reporter d'un an le roulement. Et donc, ce que cela vous montre, c'est que plus on a de données, moins on se pose des questions par rapport à ce que nous disent ces données. Il y a eu un pic pour le roulement de KSK qui nous indique qu'on a un pourcentage supérieur de résolveurs qui étaient au KSK 2010. Ensuite, donc cette bosse, ce pic s'est éliminé maintenant.

Donc ceci, je vous le montre pour simplement vous montrer que l'on continue de surveiller. Vous pouvez vous rendre sur le site Web. Nous allons continuer de publier ces données. Mais je crois que cette valeur n'est pas forcément fiable ; c'est simplement, bon, quelque chose qui est intéressant dans le domaine de la recherche.

Donc comme tout le monde le sait sans doute, il y a eu très peu d'impact selon ce que nous avons pu observer en termes de

roulement de la KSK. Juste un petit rapport de problèmes qui a été envoyé à l'ICANN, et il n'y a eu que vraiment quelques problèmes isolés. Une personne qui a dit oui j'ai quelque chose qui n'a pas marché ; je me suis rappelé qu'il y avait le roulement de KSK et j'ai réparé le problème.

Il y a eu quand même deux pannes qui peuvent être un résultat du roulement de la KSK. En Irlande, une FSI a parlé d'une panne. Alors c'était assez étrange. Je ne pense pas que ce soit lié au roulement de KSK. Je ne sais pas.

J'ai refait cette présentation à plusieurs reprises, et j'espère qu'un jour ou l'autre, ils vont nous répondre et nous dire si vraiment c'était lié au roulement de la KSK. Simplement ce qui m'intéresse, c'est de savoir le détail. Si c'était lié, j'aimerais savoir quelles sont les raisons.

Et puis dans le Vermont, je me suis également adressé à eux, et ils m'ont dit qu'ils allaient me répondre. Donc on va voir si c'était une panne liée au roulement. Donc si j'avais un membre de l'équipe ici, il me rappellerait que le KSK n'est pas terminé ; il y a encore du travail.

Donc lors de la cérémonie, nous allons gérer la signature qui révoquera la clé 2010. Ce sera le 11 janvier. C'est le moment où on va publier la zone racine avec l'ensemble révoqué KSK 2010, et la signature supérieure fait partie du RFC 5011. À ce moment-là, au moment de la révocation, il faut qu'il y ait autosignature pour publication de la clé privée. Donc cela veut dire qu'on aura une réponse DNS key plus importante dans la zone racine.

Nous n'avons pas d'indication comme quoi il y a de réponse DNS key plus large. Je crois que c'était le 11 janvier 2017 que nous avons publié quatre DNS key de KSK de zone racine pour la première fois. Donc il n'y a pas eu de problème qui était signalé à ce niveau-là. Et donc je pense qu'on n'aura pas d'autres pics. Et ensuite le 22 mars, c'est là qu'on va retirer la KSK 2010 de la zone racine, donc à ce moment-là on aura une seule KSK, deux ZSK, lorsqu'on fera le roulement de clé. On n'a toujours pas terminé. Les matériaux clés pour la KSK 2010 demeurent sur le HSM utilisent l'ICANN, donc on les effacera aux troisième et quatrième trimestres.

Donc voilà. Dernière diapositive. Je n'ai rien d'autre à dire par rapport à l'avenir si ce n'est que maintenant nous avons pratiquement terminé le roulement de clé, et donc on peut commencer la discussion. Et je vais répéter ce que j'ai déjà dit. À l'ICANN, nous travaillons avec la communauté sur ce roulement de KSK sur l'avenir parce que ce n'est pas à nous de prendre la décision de manière unilatérale. Nous travaillons avec la communauté. Je pense que l'idéal, ce serait de présenter une proposition initiale pour lancer la discussion. Sinon, on va avoir tout un tas de suggestions de différentes personnes et ça n'a jamais terminé.

Donc il y a plusieurs choses dont il faut parler : la fréquence des roulements de KSK, est-ce qu'on souhaite une KSK d'attente standby, les algorithmes. Toutes ces questions sont liées et séparées en même temps. Donc il nous faut voir comment cadrer la discussion, parler à la communauté de manière à ce que la discussion soit productive. Donc je crois que bientôt, d'ici Kobe, on pourra lancer la discussion. Et voilà,

c’est tout pour ma présentation.

RUSS MUNDY : Merci beaucoup, Wes. Merci, Matt. Merci beaucoup pour ces présentations. Et nous sommes à l’heure. Je m’excuse de ne pas avoir le temps pour avoir du temps pour répondre aux questions, mais je vous rappelle que le déjeuner ici préparé, ce n’est pas pour nous. Nous, on va déjeuner au deuxième étage. Il faut prendre deux escalators. N’oubliez pas vos tickets-repas.

[FIN DE LA TRANSCRIPTION]