ABOU DABI – Atelier sur les DNSSEC - 2e partie
Mercredi 1 novembre 2017 – 10h30 à 12h00 GST
ICANN60 | Abou Dabi, Émirats arabes unis

ORATEUR NON-IDENTIFIÉ: Nous sommes le 1er novembre 2017. Il s'agit de la deuxième partie de l'atelier DNSSEC. Il est actuellement 10:30 du matin à Abu Dhabi.

RUSS MUNDY : Très bien, on va commencer.

Très bien donc nous allons recommencer notre programme avec cette seconde partie de notre atelier, et nous avons notre panel. Nous allons changer un petit peu l'ordre des présentations par rapport au programme qui vous avait été remis.

Ah ! Duane est là, je ne le voyais plus. Venez donc plus près de nous, Duane. Vous serez ainsi plus visible. Voilà, installez-vous là. Très bien, merci.

Donc, l'ordre de présentation révisé sera le suivant : nous allons commencer par Duane, puis par Jaap Akkerhuis, puis Cristian Hesselman, Geoff Huston et nous terminerons avec Roy Arends de l'ICANN.

Je crois que nous avons assez de temps pour toutes ces présentations mais je peux vous demander de ne pas trop traîner parfois, pour que nous ayons assez de temps pour poser des questions et obtenir des réponses de la part de nos intervenants. Donc nous prendrons des questions à la suite de chaque présentation. Et sans plus attendre, je vais donner la parole à Duane Wessels.

DUANE WESSELS : Oui. Je passe en premier pour vous donner un petit peu des informations sur le point dont nous allons parler ce matin. Cette présentation est au sujet du RFC 8145 et du rapport avec le roulement de la clé KSK et le signalement des ancres de confiance. J'ai déjà donné cette présentation au DNS-OARC, c'est donc assez similaire. Voilà.

Donc en ce qui concerne ce document RFC 8145, signaler les ancres de confiance et la connaissance des ancres de confiance dans le cadre des extensions de sécurité de la DNSSEC. Je vais expliquer un petit peu comment cela fonctionne.

Le signal a une étiquette, une clé. On identifie des clés. Il y a deux valeurs qui nous intéressent aujourd'hui : 19036 pour la KSK de 2010 ou pour la clé de 2010 ; et pour la clé cryptographique de 2017, nous avons la valeur 20326. Les

serveurs des différentes zones sont reportés, il y a une transition qui doit être effectuée dès que la clé du DNS expire.

Donc le signalement de ces clés, nous avons une option 0. Cela n'a pas encore été mis en place par qui que ce soit donc toutes les données sont séparées. Nous avons une autre option, un deuxième format. Nous avons simplement une demande séparée qui est faite et les valeurs sont encodées en présentation hexadécimale de ces clés. Donc vous avez le 4a5c par exemple.

Donc voilà un petit peu le calendrier et les mises en œuvre de cela pour ce qui était de ce roulement de la clé. En 2016, il y a eu une première mise en œuvre avec BIND. Par la suite, nous avons le document RFC 8145 en avril 2017, et il y a eu une mise en œuvre dans Unbound. Et en mai 2017, nous avons commencé à collecter des données.

Dons dans BIND, par défaut, c'était sur « oui ». Et au début, pour Unbound, cela n'a pas été mis sur « non » mais cela a été changé au 1er octobre 2017 par défaut. C'était le « oui » qui avait la priorité.

Donc au sujet des données et des sources de données, comme je l'ai dit auparavant, les signaux sont envoyés aux serveurs de la zone racine, racine-A et racine-J. C'est important. Ces données proviennent donc d'une mise en œuvre récente d'un logiciel et

c'est seulement pour les personnes qui ont mis à jour récemment leur logiciel que cela se fait.

Donc un petit échantillon de données que vous avez sur l'écran. Voilà à quoi cela ressemble. Vous avez des colonnes en bas et vous avez donc par UNIX des dates et vous avez TA-4a5c qu'on avait vu à l'heure, et ainsi de suite. Donc voilà comment c'est codé avec la date, enfin, sur la droite. Voilà comment les données sont collectées.

Et nous vous montrons les anciennes ancres de confiance. Certaines possèdent également les deux valeurs. Ça, ce sont des sources qui sont déjà passées par le roulement de la KSK, de la clé cryptographique.

Donc voilà le nombre de sources fournissant les données, le nombre d'adresses IP par jour au début de mai, de mai à novembre. Vous voyez, au niveau vertical, sur la gauche, on a publié sur la zone racine la KSK 2017. Et la deuxième ligne verticale sur la droite indique le moment, le temps. Et vous voyez à quel point se termine donc le RFC 5011, et donc à quel moment la nouvelle clé est mise avec les ancres de confiance. Donc on a eu 500 sources par jour à peu près, et on était jusqu'à 2500 par jour très récemment.

Donc voilà le type de signaux qui sont envoyés. Cela, c'est est par jour. Donc vous avez en rouge sur la gauche les signaux

indiquant uniquement les ancres de confiance 2010. En vert, vous avez des sources signalant à la fois 2010 et 2017 au niveau des ancres de confiance. Et c'est un petit peu difficile à voir, mais entre le rouge et le vert, il y a un petit peu de jaune qui est difficile à voir sur l'écran. Ça, ce sont des sources qui parfois, durant la journée, envoient des signaux un petit peu mixtes. Parfois, ils envoient des ancres de confiance 2010 et parfois, 2010 et 2017, l'ancienne et la nouvelle clé ; mais c'est un petit pourcentage.

Donc ce qui nous inquiétait pour le roulement de la clé, c'est que durant le temps de latence un petit peu, on n'avait pas de baisse de ce nombre de signaux qui étaient envoyés. Et vous pourrez noter sur la gauche que nous avons une remontée légère. Voilà comment on peut vous le présenter également. Ça, c'est la même donnée mais représentée comme un pourcentage plutôt qu'en chiffres ou en nombres. Là, vous avez... Donc à la fin de la période, beaucoup – et lorsqu'on est passé donc d'une période à une autre au niveau des clés, vous voyez comment cela s'est déroulé au niveau des signaux envoyés.

Je n'ai pas donc la possibilité de vous le montrer sur le diagramme mais vous voyez sur la droite, à la fin du mois d'octobre, vous voyez que ça augmente un tout petit peu. Premières indications, cela est dû à Unbound. Unbound, vous savez, le 10 octobre, a lancé une version qui permettait le

rapport des ancres de confiance par défaut, avec le « oui » donc. Et il semble que ce peuplement, donc, dans ce peuplement, il n'y avait pas toujours la nouvelle clé. Donc merci. Très bien.

C'est intéressant également lorsque l'on voit les données qui sont non-IANA. Depuis les débuts de la collecte de données, nous avons observé que 29 tags ou étiquettes pour la racine autre que 19036 et 20326, il y a un mois, on était à 19. Maintenant, on est passé un petit peu en haut, cela a été 29, et c'était une centaine d'adresses IP de sources distinctes par jour.

Donc vous voyez un petit peu cette augmentation sur la droite sur le diagramme. Vous voyez comment cela a été effectué. Moi, je crois que cela a été fourni par le logiciel Unbound mais la ligne bleue est en hausse parce que, me semble-t-il, certaines populations et moteurs de recherche et systèmes d'opérations ont ajouté la zone racine DSK aux ancres de confiance. Donc cela ne cause pas problème, mais ça, c'est représenté sur le diagramme, parce qu'on n'est pas sûr exactement du pourquoi de cette remontée.

Donc les conclusions de ma présentation. Les signaux de BIND sont d'une assez bonne qualité et il n'y a pas eu de problèmes de données mauvaises ou néfastes, des problèmes de ce type. Nous avons des protocoles internet dynamiques. Nous avons donc une vue uniquement partielle. Cela complique beaucoup notre

analyse. Il y a également des transferts de données qui sont effectués. Je crois que Roy va entrer un peu plus dans les détails à ce sujet. J'ai déjà mentionné la date du 10 octobre. On ne sait pas très bien ce qui s'est passé à cette date, de nouveaux signaux qui sont apparus.

J'aimerais remercier beaucoup ISC pour avoir mis en œuvre cela. Et j'aimerais remercier également NLnet Labs qui nous permis de mettre sur « oui » par défaut ce signalement des ancres de confiance, ce qui est très important. Et c'est donc important de mettre en place ce document RFC.

Je suis maintenant prêt à répondre à vos questions.

RUSS MUNDY : Oui, quelques question. Nous avons le temps pour répondre à quelques questions. Allez-y, Ondrej ?

STEVEN BARRY : Je suis de .ca. Vous avez noté que pour Unbound, il y a eu une augmentation, un moment, des signaux. Le nombre relatif lorsqu'on compare Unbound et BIND, cette différence qui existe ?

DUANE WESSELS : Oui, alors, je n'ai pas eu le temps de mettre tout cela sur ma présentation, mais nous avons également des diapositives qui nous indiquent comment on sait cela. BIND fournit des signaux à des intervalles réguliers de 24 heures. Et Unbound – j'ai les deux à la maison – donne les données moins régulièrement et avec des intervalles plus courts. Donc cela, on l'observe avec ces données. C'est pour cela que j'ai associé cela à un problème de signaux. Je n'ai pas les chiffres exacts. C'est 5-10 % à peu près.

ONDREJ SURY : Merci de votre présentation. C'était très intéressant. Nous venons de mettre en place cela hier, donc c'est tout à fait intéressant pour nous. Et nous allons soutenir cette fonctionnalité très rapidement donc.

DUANE WESSELS : Merci beaucoup. C'est tout à fait positif.

ROY ARENDS : Petite question rapide : est-ce que vous savez, Ondrej, quand sera la prochaine sortie et mise à jour ?

ONDREJ SURY : Non, je ne sais pas exactement. Vous savez, on n'a pas encore fait tous les tests, donc a besoin de faire plus de tests avant de

passer à la version suivante. Donc nous ferons le maximum pour aller vite.

RUSS MUNDY : Allez-y.

ROY ARENDS : Point de clarification, s'il vous plaît. On en a parlé hier. Vous nous dites si on n'est pas dans le 40356 et l'autre numéro en ce qui concerne ces étiquettes 4a5c, cela veut dire que les signaux que nous avons observés vont vers ces deux clés. Est-ce exact ?

DUANE WESSEL : Oui, c'est exact, oui. Je reviens sur ma diapositive. On s'attend à voir la clé attendue et celle qui n'est pas attendue. Donc en bleu, cela indique des signaux qui donnent les deux clés. En rouge, et c'est tout en bas, c'est à 0, c'est une clé dont on ne s'attendait pas à la voir apparaître.

RUSS MUNDY : Donc j'espère que nous avons eu le temps de répondre à vos questions. Nous vous félicitons pour cette présentation.

Et nous allons maintenant passer la parole à notre prochain intervenant, Jaap Akkerhuis.

JAAP AKKERHUIS : Merci. Nous aussi, nous avons utilisé Unbound entre autres.

Je vois, d'après la présentation de Duane que le signal que l'on obtient est très difficile à interpréter. Il se pourrait que les clés ZSK ne soient pas toujours bien mesurées. Bon, enfin.

On ne parle pas souvent de Unbound et de ce qui se passe pour les vendeurs. Si vous êtes en train de mettre en ouvre des logiciels ou des fonctionnalités que vous ne connaissez pas bien, ce n'est pas facile.

Donc en termes généraux, nous avons des nouvelles fonctionnalités dans le DNS. Donc nous sommes plutôt conservatifs au niveau des politiques. Lorsqu'on a des versions préliminaires de l'internet qui sont lancées, nous ne sommes pas sûrs si cela va durer ou pas, et que nous voyons des spécifications qui ne sont pas stables, nous délibérons des différentes versions et du temps que cela nous prends d'agir dans des appels de conférences. Donc on évalue la faisabilité de l'application de ces nouvelles fonctionnalités pour nous. À mesure que les nouvelles fonctionnalités se stabilisent un peu, nous les lançons, mais en tant qu'options de temps de compilation, c'est-à-dire que nous donnons aux personnes le temps de savoir quoi faire. Au départ, les personnes ne savent

pas quoi faire, donc il faut qu'ils fassent du travail supplémentaire pour arriver à comprendre de quoi il s'agit.

À l'IETF, nous avons une allocation de 48 heures pour pouvoir agir comme choix de temps hors ligne. Les 48 heures, c'est vrai qu'en termes IETF, cela équivaut des fois à quelques mois mais en tout cas, nous commençons à travailler sur le lancement de cette fonctionnalité comme option de runtime. Et les personnes ont donc le choix de commencer à l'utiliser si elles savent comment le faire.

Alors lorsque les normes sont vraiment publiées en tant que RFC suite à cette période de 48 heures, nous reprenons ce que le RFC recommande et nous le publions en tant que configuration par défaut. Lorsque cela implique de grandes modifications, des fois, nous attendons à une deuxième publication mais cela reste une nouvelle fonctionnalité. C'est pourquoi nous essayons de le faire automatiquement, par défaut. Donc voilà la politique. Je sais qu'il y en d'autres qui font comme nous.

Alors, dans le cas du 5011, au départ, c'était lancé comme un programme indépendant sur Unbound. Cela s'appelait l'ancre de Unbound, qui est complètement différent de ce qu'il est en ce moment. Donc c'était un programme séparé et indépendant avec lequel les personnes pouvaient jouer et cela n'avait aucun impact ailleurs. Mais à la fin de la période des 48 heures, cela a

été intégré à la base de données principale. Et donc, nous avons commencé à travailler avec Unbound déjà en 2009, avant qu'ils deviennent la norme officielle, même avant le déploiement du DNSSEC dans la zone racine.

Le problème, c'est que ce n'est pas un protocole comme tel. Le 5011 est un document. Cela ne vous dit pas quoi faire, cela vous dit comment le faire, comment faire les choses. C'est-à-dire que les tests sont très compliqués à suivre. Vous voyez ? Cela fait quelques années que nous avons commencé à travailler sur un cadre uni-test, le but est de pouvoir faire des essais sur certaines fonctionnalités avant qu'elles soient publiées et divulguées.

Et alors, pour le 5011, aussi, nous avons créé un cadre de tests. J'ai fait mes diapositives à la dernière minute donc le texte n'est pas correct ici. Donc nous avons créé un échafaudage de test de DNS pour accélérer les temps. Ainsi, nous avons eu la possibilité d'accélérer un peu les délais par la suite, pour pouvoir donc nous conformer à la période de temps qui nous était allouée d'après le 5011. C'était [inintelligible] qui a créé cet échafaudage, comme je l'ai dit, de tests pour le DNS. Ils ont élaboré et développé des tests génériques qui ont été publiés en vrac.

Après 2009, nous avons commencé à voir des changements croissants, c'est-à-dire qu'il y avait d'autres fonctionnalités qui

étaient également déployées, et donc on voyait des changements pour répondre au 5011. Mais en définitive, il n'y a pas eu de modifications essentielles. C'était pour résoudre les bugs. Donc nous faisons nos essais sur le 5011 depuis 2009, mais cela nous a pris un moment.

Par la suite, nous avons créé des cadres de tests accélérés. Rick Lamb a créé le Rick-Roll, et puis Warren Kumari a créé un key rollerover, qui était deux roulements constants. Et Rick le fait toutes les 90 minutes. Vous voyez ? Donc c'est rapide. Cela dépend des jours, bien sûr. Mais pour faire nos tests vis-à-vis des tests de référence, on a fait recours à Unbound pour pouvoir suivre ce protocole faux. À ce moment, on a commencé à voir d'autres problèmes parce que cela rajoute des arrêts qui ne sont jamais utilisés. C'et ce qu'on appelle des [inintelligible]. Et ceux vont être utilisés ne seront jamais testées. Donc ce ne sont que des simulations en définitive. Il fallait donc apporter des modifications au code pour utiliser ces références. Et parce qu'on était tellement occupé, on n'a pas pu suivre les cas principaux. C'est ce qu'on appelle un corner case en anglais.

Alors pour commencer à faire le DNSSEC, on devait respecter les périodes d'attente de 30 jours. Mais comme on commençait à peine, on ne savait pas très bien quoi faire. Strictement, le Unbound suivait le protocole au mot à mot, et donc ce n'était pas facile. BIND disait tout simplement « Voilà le roulement,

passons à une certaine date et puis c'est tout. » Ils n'ont pas pensé à faire des tests plus avancés. Mais dans ce cas-là, nous avons remarqué que cela se faisait sans spécification au niveau des protocoles. Il y a beaucoup de personnes qui ont travaillé sur Unbound pour faire leurs essais et qui ne suivaient donc pas toutes les régulations des cas de référence. Ils pourraient faire le 5011 ou pas, ce qui est difficile.

Donc si vous faites le travail sur le DNSSEC, si vous l'avez fait dans les 30 jours, vous avez vu que si vous étiez dans cette situation, vous n'aviez qu'à supprimer l'ancienne ancre et redémarrer Unbound, ce qui aurait bien fonctionné, parce que 5011 fait la même chose. De toutes façon, les régulations d'Unbound suivent cet exemple en ce moment. Donc cela revient au même. Voilà ce que je dis ici. Si vous avez utilisé l'ancienne clé de signature de clés, tout aurait bien fonctionné aussi. Ce n'était qu'une question de redémarrer le serveur. C'est cela que je dis ici.

En fait, le problème était qu'on n'a pas vu, qu'on n'a pas su voir en tout cas, les impacts que ce aurait faits. Tout était une grande expérience en définitive. Et je sais que ce sera remplacé sous peu, sans doute. Merci.

RUSS MUNDY : Merci Jaap. On a le temps de quelques questions. S'il y a des questions rapides, on pourra y consacrer quelques minutes, si vous voulez. Je ne vois pas de main levée. Est-ce qu'il y a des questions en ligne ? Bien. À ce moment-là, Jaap, nous vous remercions.

Maintenant, nous avons Cristian Hesselman sur le projet de Root Canary.

CRISTIAN HESSELMAN : Vous m'avez consacré 23 minutes. Je ne pense pas que ça aille me prendre autant de temps.

En tout cas, je viens vous parler d'un projet qui s'appelle Root Canary, le canarie de la racine, pour quantifier la qualité de la validation du DNSSEC. On a travaillé avec deux universités, NLnet Labs, Surfnet, et SIDN Lab ainsi que RIPE NCC, bien sûr.

Le projet Root Canary est également connu comme le canarie dans la mine virtuelle (Canary in the Virtual Coalmine). Vous savez que de par le passé, les personnes qui travaillent dans des mines amenaient toujours des canaries pour se rendre compte s'il y avait des problèmes avec le monoxyde de carbone dans la mine parce qu'à ce moment-là, le petit oiseau mourrait. Donc c'est un peu similaire, mais c'était appliqué au roulement de la KSK. C'était fait pour évaluer l'impact du roulement de la KSK

dans la racine, et cela nous aurait indiqué s'il y avait eu des problèmes. Mais en même temps, on voulait également mesurer la validation au cours du roulement de la KSK d'un point de vue global pour apprendre de ce type d'évènement. Donc c'était cela les deux buts principaux de notre projet.

À la base, il s'agit d'une méthodologie de mesures que nous avons utilisée à travers quatre perspectives différentes. Les deux principales sont RIPE Atlas et Luminati. RIPE Atlas est un réseau européen de capteurs qui ont des nodes de réseau, à peu près 4 000, qui sont éparpillés partout sur la planète. Et donc cela dépend surtout des réseaux des personnes chez elles, dans la maison. Donc partout sur la planète. Et puis Luminati est un réseau de proxy que les personnes utilisent pour cacher leur adresse IP. Nous sommes en train de négocier avec APNIC également pour voir si nous pouvons utiliser leurs mesures dans notre méthodologie actuelle. Et nous considérons également la perspective hors-ligne, c'est-à-dire que nous ferons des mesures du trafic au niveau du serveur de la racine sans connectivité une fois que le roulement aura déjà été complété. Donc c'est un projet de mesures.

Suivant cette même méthodologie de mesures, nous avons signé certains noms de domaine, certains qui ont des signatures valides et d'autres qui ont des fausses signatures. Et ce que nous essayons d'obtenir à partir de ces informations est un numéro

qui nous permette de savoir quelle est la quantité de résolveurs qui font la validation correctement, ce qui nous donnes les échecs au niveau de la validation et les résolveurs qui ne valident pas du tout. Et dans le cadre de ce projet, nous mesurons également quels sont les validateurs qui supportent quel type d'algorithme.

Voici le réseau Luminati dont je parlais. Il s'agit d'un service d'enregistrement fiduciaire https, un service proxy https qui fonctionne avec RIPE Atlas. Donc ils comprennent 15 000 systèmes autonomes sur lesquels 14 000 ne sont pas couverts par RIPE Atlas parce qu'en général, les réseaux sur RIPE Atlas ont d'autres fonctionnalités. Donc tout cela appartient au réseau des consommateurs finaux en général. Il pourrait donc être plus représentatifs de ce qu'il se passe, ou en tout cas, plus que ce que nous voyons sur le réseau RIPE Atlas

Donc nous avons fait quelques mesures le 19 septembre. C'était le moment où il y avait une augmentation des chiffres pour la clé du DNS. Donc voilà une réponse que nous avons lorsqu'il y a des problèmes avec les serveurs, les différents types de réponses SERVFAIL. Désolé, il y a des erreurs typographiques sur cette diapositive. C'est historique cela, voilà.

Ça, c'est l'utilisation de TCP et UDP pendant cette période sur la racine P. Donc si quelque chose d'un petit peu bizarre se passait,

et bien les résolveurs seraient passés au TCP puisqu'ils ont un accroissement des messages et du nombre de messages. Cela ne s'est pas véritablement passé, donc c'est intéressant. Et ça, c'est les résultats préliminaires de fragmentations. Pas beaucoup de changement au niveau de la fragmentation. Donc rien ne s'est encore déroulé puisqu'évidemment, on a remis à plus tard le roulement de cette clé cryptographique KSK.

Mais en général, nous voulons utiliser cette méthodologie pour l'infrastructure et mesurer donc, au niveau des TLD, ce roulement de clés. Je crois qu'il faut bien avoir plus d'informations sur les résolveurs, comment ils jouent leur rôle, mesurer l'utilisation des algorithmes du DNSSEC. Mais nous devons, évidemment, passer par le véritable roulement de la clé KSK.

Donc vous pouvez tout à fait nous aider si vous faites des mesures sur vos réseaux, sur vos propres machines informatiques. Vous pouvez collaborer à cet effort en utilisant ce script small shell. Et vous pouvez faire des requêtes, des demandes par défaut avec les résolveurs toutes les heures, donc faire des tests sur vos réseaux. Voilà plus d'informations, il y a une page web, il y a des tests d'algorithme pour notre projet Root Canary.

Voilà, c'était mon dernier transparent. Nous avons les résultats pour RIPE et vous voyez, tous ces liens hypertests que vous pouvez accéder.

RUSS MUNDY : Nous pouvons maintenant remercier notre intervenant et s'assurer qu'on est bien réveillé. On a des questions pour notre participant sur le canarie ? Allez-y, Roy.

ROY ARENDS : Bonjour. Vous avez mentionné et vous vous êtes corrigé. Je n'ai pas bien compris. Je crois qu'il va y avoir très bientôt un nouveau script. [inintelligible], vous mesurez l'accroissement de cela ?

CRISTIAN HESSELMAN : Oui, l'accroissement du nombre de messages.

ROY ARENDS : Donc avec Verisign, nous sommes partenaires pour ces tests ; on les faits tous les trois mois. Donc ils effectuent cela annuellement.

CRISTIAN HESSELMAN : Très bien, d'accord. Je prends note.

RUSS MUNDY : Oui ?

ORATEUR NON-IDENTIFIÉ : En ce qui concerne vos algorithmes, vous vérifiez les algorithmes dans un projet canarie. Est-ce que vous avez des données obtenues, par pays par exemple ? Comment les algorithmes sont soutenus ?

CRISTIAN HESSELMAN : Oui, nous avons pas mal de données à ce sujet mais je n'ai pas inclus cela dans ma présentation. Mais c'est sur le site web rootcanary.org. Donc allez voir, vous avez beaucoup de tests sur les algorithmes sur cette page web.

ORATEUR NON-IDENTIFIÉ : Très bien.

JAAP AKKERHUIS : Donc on voit les mesures en temps réel. Cela prend beaucoup de temps de computation et de gestion de l'information. C'est assez lourd.

ORATEUR NON-IDENTIFIÉ : Oui, je vois sur le site web que.., Est-ce que cela inclut également les données de Luminati ?

CRISTIAN HESSELMAN : Bonne question. Je ne suis pas sûr, à savoir si les données de Luminati sont présentes là-dessus.

RUSS MUNDY : D'accord. Une autre question ?

JAAP AKKERHUIS : Donc j'avais apporté cinq exemplaire avec moi de ce processus d'échantillonnage. On a vraiment besoin de faire plus de tests dans cette région du monde. Donc n'hésitez pas à venir me voir pour que je vous remette un de ces exemplaires.

RUSS MUNDY : Merci beaucoup.

Nous allons maintenant passer à Geoff Huston qui va maintenant présenter. Nous allons mettre sa présentation sur l'écran. Geoff, comment allez-vous ?

GEOFF HUSTON : Bonjour à toutes et à tous. J'attends donc que la première... Cela, ce n'est pas la bonne présentation.

ORATEUR NON-IDENTIFIÉ : Mais c'est pourtant votre présentation, Roy. Roy Arends qui est donc de l'ICANN, qui est scientifique.

GEOFF HUSTON : Oui, peut-être qu'elle est un petit peu vieille ma présentation. J'en avais envoyé une il y a de cela quelque temps. Elle est un peu moisie peut-être.

Alors mesurer, donc, si on est prêt au roulement de la clé cryptographique KSK. Donc je contrôle très bien, je contrôle les diapositives. Cela ne s'affiche pas très bien. Voilà, c'est mieux.

Les objectifs donc de ces mesures. La grande question qui se posait pour l'ICANN, pour la gestion de ce roulement de clé KSK, le grand problème, c'est quel était le nombre d'utilisateurs qui sont à risque, qui connaissent un risque d'être impacté par cela. On sait qu'il y a environ 11 à 12 % des utilisateurs pour faire la validation DNSSEC. Et donc cela poserait des problèmes de validité. Ils n'ont pas fait la validation DNSSEC et ils n'auront pas la possibilité d'utiliser des résolveurs. Donc beaucoup d'utilisateur, 12 % environ, pourraient potentiellement être affectés par un roulement de clé KSK qui se passerait mal. Donc voilà ce qu'on a pu mesurer.

Maintenant, il y a deux éléments de risque. Premièrement, c'est la première fois avec une réponse assez large qui fait partie intégrante de résolveurs de validation, parce que les réponses qu'on obtient principalement, c'est 1440 octets, une réponse UDP de la part des serveurs de la zone racine. De facto, on utilise IPv4 à ce niveau. Le problème, c'est qu'avec ce chiffre arbitraire de 1280 qui est utilisé, et bien, pour arriver à 1440 octets, qu'est-ce que cela veut dire ? Pas grand chose. Donc on en est toujours à 1280 et il y beaucoup et c'est un peu bizarre, mais il y a beaucoup de chiffrage qui sont à 1280. Donc ça, c'est une question de fragmentation IPv4 et IPv6 qui nous pose problème.

Donc comme vous l'avez entendue, vous avez la question du RFC 5011. On ne peut pas tester la production, on ne peut pas suivre, donc, cette introduction de la clé. On ne peut pas tester cela dans un environnement de production. Donc si vous connaissez des ratés, vous avez de sérieuses ratés et on revient avec les même résolveurs, on ne peut rien faire, tout simplement. Et c'est une perte de service. Donc le résolveur ne va plus faire son travail, ne va plus servir et donc toute une zone pourrait connaître une panne. Et l'on parle de 11 à 12 % des utilisateurs de l'internet.

En ce qui concerne la possibilité de mesurer les résolveurs. On a parlé des utilisateurs, on a parlé des résolveurs. La manière dont cela fonctionne, c'est qu'ils soutiennent un mécanisme de signal

périodique. Allons un petit peu plus loin. Uniquement les serveurs de la zone racine voient ces signaux, et ils sont transférés ; personne d'autre ne le voit. Donc c'est un signal qui n'est pas secret mais c'est très difficile de le retrouver, ce signal, et de retrouver sa trace. C'est une requête sans attribution. Donc si vous transférez, et bien je deviens invisible en quelque sorte. Il y a des signaux qui deviennent invisibles parce qu'ils sont transférés. Et cela prête beaucoup à confusion par rapport à l'attribution du signal.

Donc dans le monde du DNS, il y a des résolveurs qui sont plus importants que d'autres. Par rapport, le service DNS public de Google fournit le DNS pour 14 à 15 % de la population mondiale. Donc leurs résolveurs sont extrêmement importants. Donc mon résolveur chez moi, c'est juste pour moi. Donc je ne dis pas que c'est sans importance, moi, j'aime bien, mais vous autres, vous ne vous en préoccupez pas.

Donc essayez de bien comprendre que certains signaux sont plus importants que d'autres par rapport au nombre d'utilisateurs. Ce n'est pas tout à fait apparent dans ces données, mais ce qui n'est pas clair non plus, c'est que si un résolveur connaît une panne, la plupart des personnes, surtout en .com, ont plusieurs résolveurs. Donc vous allez recevoir peut-être une réponse de B. Pas de problème, vous allez passer de A à B, donc les utilisateurs vont pouvoir s'y retrouver. Mais mesurer

les résolveurs par la même ne suffit pas pour répondre aux questions qui nous sont posées. Ce n'est pas la bonne réponse. Ce que vous voulez, obtenir les données que vous recherchez.

Donc il faut trouver une requête du DNS qui peut révéler l'état des ancres de confiance, des clés de confiance dans le résolveur. Il ne faut pas être victime de son service DNS. On se base sur des résolveurs. Il faut qu'ils continuent à fonctionner. Donc est-ce que l'on peut effectuer ce type de requête, effectuer ce type de requête ? La réponse, c'est non, on ne peut pas, on n'y arrive pas, ce n'est pas possible. Peut-être certaines personnes pourraient trouver un moyen mais je ne crois pas que ce soit possible. Pour le moment, tout le monde se pose la question. Quelque chose doit changer. Au niveau des domaines du DNS, est-ce qu'on doit changer quelque chose ? Des nouveaux paramètre, peut-être ? Ce n'est pas dans les cadres des paramètres actuels de DNSSEC. Ou peut-être faudrait-il changer le comportement de ces résolveurs ?

Donc on a noté cela, avec Unbound, avec NSC, on a vu qu'il y a des changements de code, que c'était possible. Mais c'est bien là le problème. Est-ce que je peux prendre une étiquette – c'est juste d'une étiquette dont on parle... Si on le met dans le nom de domaine, est-ce qu'avec un résolveur de validation, vous allez pouvoir changer et connaître des problèmes ou pas ? Donc dans le premier cas, est-ce que cette étiquette et cette ancre de

confiance, est-ce que vous allez recevoir une réponse ? Est-ce que vous allez avoir un code 3 ? Est-ce que vous allez avoir une panne de serveur ? Est-ce que vous pouvez faire confiance à cette clé ? Parce que nous devons détecter la différence entre les résolveurs qui soutiennent ces mécanismes et ceux qui ne soutiennent pas. Vous devez également faire l'inverse. Ce n'est pas une clé à laquelle on peut faire confiance.

Donc trois requêtes pour le DNS. Vous pouvez faire cela, vous pouvez faire vos propres tests en tant qu'utilisateur à some.signed.domain. Et mettez une étiquette qui est mal signée, avec une mauvaise signature. Donc essayez de créer un défaut, un problème. Si vous regardez le type de réponses que vous obtenez, il y a quatre types de comportements de résolveurs. On soutient le nouveau mécanisme et télécharge la clé de roulement. Donc vous voyez, lorsqu'il y a une panne de serveur SERVFAIL ou lorsque tout se passe bien. Donc vous voyez sur l'écran quels sont les différents cas de figure, est-ce que le nouveau mécanisme est supporté ou pas.

S'il n'y a pas de validation, là, on a A-A-A. Donc je peux distinguer les quatre cas qui m'intéressent véritablement. Et vous n'avez pas qu'un seul résolveur, vous en avez plusieurs. Et en général, ils font des transferts, c'est très complexe. Mais l'analyse des résultats est assez similaire. Si je reviens à tous mes résolveurs récursifs, cela va. Si j'ai SERVFAIL pour le deuxième et SERVFAIL-

SERVFAIL, cela veut dire que ça va. Si vous commencez par un SERVFAIL, cela ne va pas marcher. Les deux autres types de réponses, dans tous les résolveurs que vous utilisez, certains ne soutiennent pas ce mécanisme et vous ne savez pas quelle est la réponse. On ne peut pas savoir à l'avance quelle est la réponse. Donc résultat inconnu. Et dans d'autres cas de suivi, vous n'êtes pas impacté et tout va bien.

Donc faites-le vous-même, utilisez une page d'accueil. Si vous connaissez une campagne de publicité en ligne par exemple, mettez-le sur voter script Java et vous pouvez mesurer plusieurs centaines de millions d'utilisateurs. Donc cela compte beaucoup pour le mécanisme et pour tant de centaines de milliers d'utilisateurs. Donc les campagnes de publicité suivent de près le nombre de personnes qui sont touchées, par exemple.

Donc on joue beaucoup avec le DNS, et il est tout à fait nécessaire d'avoir un certain respect de la vie privée et de sécurité. L'identité des utilisateurs ne doit pas être révélée. Toutes les informations ne doivent pas être identifiées. Vous n'avez pas besoin d'identifier les utilisateurs. Il ne faut pas passer de « insecure » à « secure ». Il faut être prudent à ce niveau-là pour assurer la sécurité du DNS et ne pas faire empirer la situation.

Donc tout le monde peut le faire, tout le monde peut faire ces tests. Ce n'est pas exclusif. Ce n'est pas seulement les personnes qui gèrent la zone racine. Vous obtenez vous-mêmes vos données et elles sont privées. Donc vous pouvez vous-mêmes faire ces requêtes DNS qui sont tellement pratiques. C'est très ouvert. Les FSI parfois se contestent, mais c'est à vous de faire ce travail.

Vous avez donc un document que je vous présente sur... je crois que cela a deux semaines d'existence, oui. Si vous vous êtes adressé au DNS, et bien vous pouvez être et jouer ce rôle de sentinelle pour détecter les clés de confiance du DNSSEC. Donc ce qui nous intéresse beaucoup, c'est une approche, je pense, tout à fait valide. Lorsque vous prenez le signal RFC, il me semble que vous avez des attributions et vous comprenez l'importance de ce signal par rapport au nombre d'utilisateurs. Ça, c'est une approche totalement différente qui parle des clés de confiance pour les utilisateurs d'une manière très holistique, très globale. Donc cela ne va pas révéler l'identité d'un résolveur individuel parce que le DNS ne fonctionne pas comme cela. Cela va révéler simplement si un utilisateur n'aura pas de problème lors du roulement de la KSK.

Donc il reste 46 secondes pour les questions.

ROBERT MARTIN-LEGENE : Robert Martin-Legene de PCH. Bonjour. J'apprécie toujours vos présentations, Geoff. Est-ce que vous avez considéré de voir l'EDNS pour tout ce qui a un impact sur les serveurs de noms et pour voir si cela fonctionne pour faire du forwarding aussi ?

Et je pense que peut-être vous auriez pu regardé si le RFC comprenait une option d'EDNS qui ne serait pas forwardé par un forwardeur ; cela vous aurait permis d'identifier des résultats.

GEOFF HUSTON : Oui, en fait, j'ai inversé la méthode : je regarde les réponses, pas les requêtes. C'est cela qui est essentiel ici parce qu'aucune de ces informations viennent de l'autorité du serveur de noms. Le forwarding, cela ne nous intéresse pas. Mais pour vous, en tant qu'utilisateur, ce qui vous intéresse, c'est de voir ce que donne ces réponses des requêtes. Donc les réponses que vous obtenez, c'est cela qui vous intéresse, c'est ce qui est important. Et les différents serveurs de la racine ne regardent pas cela. Ils connaissent l'état de leur propre clé mais ils ne savent pas quels sont vos résolveurs. C'est vous qui savez quels sont les résolveurs que vous avez chez vous. Donc ces tests sont pour vous, pas pour la zone.

Ici, je sais qu'on a le responsable informatique, le bureau du CTO, qui s'occupe des résolveurs et c'est des problèmes qui vont affecter la racine qu'ils regardent, mais pas cela ; ils ne

regardent pas vos résolveurs. Donc pour nous, ce qui est important, c'est la réponse, pas les requêtes.

ROBERT MARTIN-LEPAGE : Oui, je comprends que c'est pour le cas spécifique que vous regardez, mais l'internet n'est pas seulement pour les utilisateurs, il y a beaucoup de systèmes automatiques. Donc s'il y a quelque chose qui ne fonctionne pas, il se pourrait que nous mettions deux mois à trouver où est le problème parce qu'en général, ces types de problèmes ne sont pas très visibles. Mais ma mère, si son ordinateur ne fonctionne pas, elle va appeler quelqu'un. C'est vrai, elle pourra vivre sans internet, mais il faut, il me semble, mesurer différents aspects aussi.

GEOFF HUSTON : En fait, ce sera susceptible de faire beaucoup de requêtes si on fait la campagne. Si on le fait bien, on pourra faire beaucoup d'échantillonnage. On ne fait pas les tests sur les dispositifs des utilisateurs ; ce n'est pas possible. On ne peut pas tester tous les dispositifs. Mais ce même mécanisme nous dit qu'entre 11 et 12 % des utilisateurs n'utilisent que la validation du DNSSEC, et donc on peut arriver au même résultat ici avec un niveau de confiance par rapport au fonctionnement de la clé KSK qui sera roulée. C'est cela, le but.

ROY ARENDS : Sur les systèmes automatisés, les personnes qui travaillent avec eux et qui les utilisent ne peuvent pas utiliser ces techniques.

RUSS MUNDY : Je pense qu'il faut qu'on avance pour que Roy ait suffisamment de temps pour faire sa propre présentation et répondre à des questions s'il y en avait. D'accord ?

Il va nous présenter ici l'état actuel de la KSK elle-même. Alors Roy, vous avez la parole.

ROY ARENDS : Me voilà à faire la même présentation pour la septième fois cette semaine. Donc je voudrais savoir à levée de main qui n'a pas vu cette présentation. D'accord, cela marche.

Alors je m'appelle Roy Arends. Je travaille dans le bureau du responsable informatique du CTO ; je suis chercheur. J'ai ici quelques informations de contexte. Je ne sais pas si vous en avez besoin. Si vous faites la validation du DNSSEC, il vous faut une ancre de confiance qui est une clé publique, qui ne peut pas durer à l'éternel, donc il faut les renouveler. Ce renouvellement s'appelle roulement en matière de DNSSEC, et cela peut être fait automatiquement ou manuellement. Mais moi et mes collègues

qui sommes là ne pouvons pas vérifier si vous avez la bonne clé configurée.

Donc au moment de concevoir ce programme il y a quelques années, nous avons vérifié les propriétés de notre méthodologie. Nous avons engagé une équipe de conception. Nous avons fait des plans, nous avons discuté avec les vendeurs, avec les gouvernements, et nous nous sommes dit que le 11 octobre 2017 était une date importante. Et c'est parce qu'à l'époque, nous ne savions pas qui faisait la validation ou pas, qui avait la bonne clé configurée et qui ne l'avait pas.

Naturellement, nous avons mis en place un processus. Le 11 juillet 2017, nous avons lancé la nouvelle clé de signature de clé KSK et nous avons contrôlé s'il y avait des changements fondamentaux au niveau du trafic dans les serveurs racines. Duane ici travaillent pour Verisign, donc il avait accès à deux racines. Nous, nous avions accès aux racines B, D, L et F. On est parvenu à avoir d'autres serveurs racines qui se sont ajoutés à notre projet aussi. Et donc il n'est pas facile d'avoir ces séances de validation de résolveurs, de faire des tests. Vous savez que si les résolveurs n'arrivent pas à faire la validation, ils deviennent très agressifs.

Il y a quelques années avec Geoff, on a fait des essais par rapport au roulement, on l'appelle roulement maintenant parce que

nous avons vu qu'il y avait des effets similaires pour les résultats de validation. C'était aussi similaire au moment de faire le changement de clé du DNS. On n'a aucun impact. Les statistiques et les graphiques sont très satisfaisants mais ils montrent une ligne droite pour le 11 juillet.

Un peu plus tard, on regardait toujours le trafic : aucun changement, donc on a continué. Nous sommes arrivé au 19 septembre et c'est de cela que je parlais tout à l'heure : Verisign, notre partenaire de gestion de la zone racine, a introduit une nouvelle clé, nous avait fait un nouveau roulement ZSK, ce qu'ils faisaient depuis 2010. Mais l'exception ici, la différence, c'était que c'était la première fois à laquelle nous avons fait augmenté la taille des réponses du DNSKEY.

Vous avez déjà vu ces graphiques dans la présentation de Duane. Jusqu'à récemment, nous n'avions pas de connaissances par rapport à la configuration des types de confiance des différentes personnes. Nous avons utilisé déjà différents RFC. On a parlé du RFC 8145, des déploiements de BIND. Donc je vais sauter cela.

On dit ici qu'on ne connaît pas d'autre déploiement mais je viens d'entendre Andre Phillip qui disait que ce ne sera plus le cas dans l'avenir. On aura une version avec la signalisation, ce qui

est très bien. Je ne suis pas au courant des récurseurs disponibles. À ce que je sache, il n'y en a pas.

Donc 4,2 millions adresses uniques envoient des requêtes au serveur racine. C'est ce que j'ai ajouté ici. C'est les valeurs que nous obtenons des serveurs racines. Mais ce doit être bien plus si l'on combine tous les serveurs racines. Si vous voulez faire une étude de la quantité d'adresses uniques, bien évidement, on en aura beaucoup plus. Donc 4,2 millions, ce n'est pas beaucoup mais c'est la limite minimale. Mais les numéros que nous avons vus à partir des données de RFC 8145 sont très faibles.

J'y arrive tout des suite... voilà. Excusez-moi. Nos statistiques vont jusqu'au 24 octobre à partir du 1er septembre. C'est à ce moment-là que j'ai dû me rendre à une réunion pour vérifier. Nous avions 27 000 adresses uniques qui envoyaient des données des étiquettes de clés sur 4,2 millions. Et 6 % d'évaluateurs qui font des rapports n'étaient pas préparés pour le roulement de KSK. Il se pourrait que ces chiffres aient changé un peu. Il faut voir si la signalisation des étiquettes de clé fonctionne ou pas. Si on le vérifiait, peut-être que les chiffres diminueraient un peu mais pas énormément.

On a déjà parlé de la complexité des analyses. J'aime bien la proposition de Geoff Huston. J'aurais bien apprécié l'avoir il y a deux ans, mais j'ai apprécié, de toute façon. C'est mon avis

personnel. Avant qu'on ne vienne me gronder, je dis c'est mon avis personnel.

Donc pourquoi la KSK-2010 a été rapporté et pas la KSK-2017 ? Avec la version la plus récente de BIND, on a des rapports des ancres de confiance même s'ils ne valident pas. C'est embêtant parce qu'on a des faux signaux. Donc on a des clés qui sont configurées et cela ne se met pas à jours parce qu'on ne valide pas.

Avant la spécification 5011, on avait une certaine configuration sur BIND avec des clés auxquelles on faisait confiance, ce qui était tout à fait raisonnable. Mais maintenant, avec le 5011, il faut changer la configuration. Cela nous permettra de vérifier que certaines clés soient mises à jour en conformité avec le 5011. Alors BIND, ce qu'il fait, c'est de gérer les clés de 5011, et il y a des personnes qui ne comprennent pas très bien comment cela fonctionne.

Je vais sauter un peu ici. On a trop de problèmes. Ce n'est pas la peine de tout vous dire.

Donc on revient au plan opérationnel. On a fait augmenter la taille aux réponses au DNS d'ici le 19 septembre, pas d'impact. Nous avons reçu le rapport de Verisign, nous avons vérifié cela avec nos propres données, mais on ne peut pas prendre des décisions ad hoc. Donc nous avons consulté le plan opérationnel

qui date d'il y a quelques années. La communauté l'a ratifié et on dit dessus que les partenaires de gestion de la zone racine, donc Verisign et l'ICANN, pourraient également décider de prolonger une étape pour d'autres trimestres. Par exemple, s'il y avait de nouvelles données qui indiquaient que l'étape suivante pourrait amener à des complications, l'étape actuelle serait prolongée. C'est ce que l'on appelle le cas de prolongement. C'est ce que nous avons fait, nous avons remis la date d'échéance et nous avons informé cela. J'ai lu quelques rapports sur certaines des listes de diffusion disant qu'il y avait des personnes qui avaient obtenu ces informations avant d'autres, mais c'est dû au fait que nos listes de diffusion et notre équipe de communication ne sont pas les mêmes que pour les personnes responsables du DNSSEC. Donc il a fallu prendre un petit moment pour faire passer le message.

Nous ne savons pas quelle est la représentativité de l'ensemble de validateurs qui nous envoient des rapports par rapport aux données des étiquettes de clés. On a dit que les validateurs ne sont pas des utilisateurs finaux. Et on a beaucoup travaillé avec Geoff. Geoff, on pourra partager davantage de données, mais les chiffres contenus dans ces rapports des données des étiquettes de clés, en fait, n'avaient aucun fondement. On avait beaucoup d'utilisateurs. J'ai entendu dire qu'il y avait 750 millions

d'utilisateurs qui avaient ce type de validateur. Ah non, pour Google, d'accord.

La mitigation est difficile. On a déjà suivi des campagnes pluriannuelles pour pouvoir essayer d'être en contact avec les opérateurs. Et les problèmes spécifiques au déploiement, bien sûr, n'aident pas. Il n'est pas possible de les isoler. Comme Geoff disait tout à l'heure, il n'est pas possible de faire ces tests dans un laboratoire. Alors nous avons remis à plus tard le roulement de la KSK de la racine, jusqu'à ce que l'on aura obtenu davantage d'information et que l'on puisse comprendre la situation un peu mieux. Ce retard durera au moins un trimestre mais on ne sait pas combien cela va nous prendre de trimestres pour y parvenir.

Les cérémonies de clé organisées par l'ICANN se font tous les trois mois. C'est pourquoi nous changeons les dates de trimestre en trimestre. Donc comme je dis, nous ne savons toujours pas combien de trimestres cela va nous prendre.

Nous allons au moins faire la mitigation partielle. Nous allons trouver un tiers qui va faire le suivi des 500 résolveurs basés sur des adresses IP pour essayer de comprendre pourquoi on a ces problèmes de configuration. Nous continuons de collecter des données.

Et par rapport à Unbound, Duane disait qu'Unbound était lancé le 10 ou le 11 octobre, ce qui coïncide avec les signaux. Il y a d'autres données qui coïncident. C'est que le 10 octobre était le dernier jour auquel on a utilisé ZSK-q3. Et c'est en raison du fait que ZSK-q3 a été ajouté au signal. Donc le fait qu'Unbound envoie cette requête n'implique pas qu'Unbound fasse la validation. Ce pourrait être un résolveur. En fait, ce pourrait être un forwardeur devant un résolveur.

JAAP AKKERHUIS : Non, mais ce signal n'arrive que lorsque cela fait la validation.

ROY ARENDS : Alors si je demande quelle est la requête d'Unbound qui utilise ces étiquettes de clés, est-ce que cela va arriver jusqu'à la racine pour poser la question pour envoyer la requête ?

JAAP AKKERHUIS : Cela va dépendre de la configuration que vous aurez. Si l'utilisateur...

ROY ARENDS : Je vais vous montrer les données tout à l'heure.

JAAP AKKERHUIS : Si on avait des forwardeurs...

ROY ARENDS : Pardon, je n'ai plus vraiment le temps. On en discutera plus tard. Je vous montrerai les données par la suite. Excusez-moi alors. Donc Unbound n'est pas toujours le problème.

Pour conclure sur cette partie-là, c'est de ne pas supprimer, je vous en prie, ne supprimez pas le KSK-2017. Parce qu'au moment du roulement, il y a des personnes qui ont décidé d'éliminer la KSK-2017, de la déconfigurer. Ne le faites pas, je vous en prie.

J'ai une autre présentation qui porte sur la fréquence du roulement de la KSK de la racine. C'était une autre présentation que j'étais censé faire au sein du groupe de travail d'experts. Il ne me reste plus qu'une minute et demie.

Donc rapidement, c'est une petite discussion sur la fréquence du roulement de la KSK. Nous avons commencé à utiliser l'ancienne clé en 2010 et nous prévoyons de commencer à utiliser la nouvelle KSK en 2018. On croise les doigts. Et les personnes qui veulent que ce soit configuré manuellement, cette nouvelle ancre de confiance, il y a des personnes qui se fondent, se basent sur la RFC 5011. Les validateurs pourraient avoir des problèmes de configuration, des partitions en mode lecture ou

qu'ils utilisent alors des paragraphes de configuration qui ne sont pas les bons. Il y a des bugs et la télémétrie de l'ancre de confiance n'est pas la bonne.

Donc on a deux écoles, lignes de pensée. Ici, on a le roulement fréquent, ce qui ne veut pas dire qu'on le fait constamment. Cela veut dire qu'on le fait à des intervalles fixes. Si on fait le roulement, rien ne se passe, on continue. C'est ce que cela veut dire.

Donc la communauté technique, il y a de cela quelques années, avait une certaine fréquence pour les roulements, tous les cinq ans. On a pensé que c'était tous les cinq ans. Donc on réfléchit bien en avance.

Moi, j'ai décidé de mettre ici une idée sur la fréquence, les cas de fréquence basse. Donc moi, je pense que cinq ans, c'est bien. Un roulement tous les cinq ans est une bonne chose. Et nous avons tous les trois mois ces cérémonies de signature de clé. C'est peut-être un petit peu ridicule selon vous, mais il y a des gens qui disent qu'il faudrait faire cela toutes les semaines. Donc c'est pour cela que j'ai mis ça sur l'écran. Trois mois à mon avis, ça va. Sinon, vous allez avoir énormément de travail ; donc un roulement tous les trois mois.

Nous avons trois étapes. Vous commencez à introduire une nouvelle clé, vous commencez la signature avec une autre clé, et

vous révoquez la première clé. Donc je ne vais pas vous parler de la deuxième ligne, mais cela peut poser des problèmes. Vous avez un nombre de bites qui est important, 1986. C'est le minimum de la taille pour la clé DNS. Donc c'est pour cela que vous devez faire une mise à jour tous les trois mois selon moi, que ce soit manuel ou semi-automatique.

Si vous le faites tous les six mois, vous n'avez pas le problème de la taille de la réponse parce que vous ne faites pas un collapse total, mais vous avez quand même deux étapes en une seule : vous introduisez clé, vous révoquez la vieille clé et utilisez la nouvelle clé. Vous n'avez que deux étapes. Vous voyez ? Mais le problème, c'est qu'on ne peut pas revenir en arrière à ce niveau. Vous devez totalement reconcevoir tout le processus. Donc moi, je crois que c'est une bonne idée de pouvoir revenir en arrière.

Ici, on a un effet d'un roulement tous les neuf mois. Là, ça ne pose pas de changement fondamental à la conception. Et ça, j'écoutais les opinions des personnes qui font ces roulements de clés. C'est notre perspective.

Il y aura toujours des problèmes, je crois, donc là, ce sera tous les quatre ans, vous aurez deux roulement de clés par an. Ce n'est pas optimal pour les opérateurs parce que ce n'est pas très prévisible.

Tous les ans : une nouvelle fois, pas de problème avec la taille de la réponse. Vous pouvez utiliser la conception actuelle du plan de roulement, c'est plus prévisible ; cela peut être une bonne chose pour les opérateurs.

Plus d'un an : pas de différence significative par rapport à un an. Donc si vous le faites tous les ans à la fin de l'année à la même date, c'est un petit peu bizarre. Mais cela veut dire avec un intervalle fixé. Moi, je crois que cela peut fonctionner et que c'est peut-être préférable pour les opérateurs.

Je sais que j'ai parlé à Jaap hier qui m'a dit – et c'est très intéressant, je pense qu'il m'a posé la question d'ailleurs – Jaap me disait : « Est-ce qu'on ne devrait pas faire un roulement de clés avant de prendre une décision ? » Il a raison. Donc on m'a forcé un petit peu à faire cette présentation, mais moi, je crois qu'on va continuer ce débat, mais on doit d'abord faire notre roulement de clés. C'est un petit prématuré de poser ces questions, « Est-ce que l'on doit changer nos délais pour les roulements de clés ? » Merci.

RUSS MUNDY : Merci beaucoup Roy.

Duane ?

DUANE WESSELS : Oui. Est-ce que l'on peut revenir sur le transparent qui indiquait à tous les six mois ? Est-ce que vous pourriez clarifier quelque chose. Vous nous avez dit il n'y a pas moyen de retourner en arrière. Une extension est-elle possible ? C'est la même chose ? Une extension, retour en arrière, je ne vois pas très bien la différence.

ROY ARENDS : Non, ce n'est pas la même chose. Je crois que si vous révoquez votre clé au moment où vous commencez à utiliser une nouvelle clé, vous ne pouvez pas revenir en arrière. Si vous attendez et ne révoquez pas tout de suite la vieille clé, vous pouvez toujours revenir en arrière.

DUANE WESSELS : Dans la situation actuelle, nous avons fait une extension de prépublication, extension de l'ancienne clé. On n'est pas passé à la prochaine étape, roulement de nouvelle clé. Donc il faudrait qu'on y réfléchisse un petit peu plus, je crois.

ROY ARENDS : Oui, on le fera.

RUSS MUNDY : Oui, je crois qu'on a vraiment abordé des problèmes très importants, me semble-t-il. Et étant donné que nous sommes un groupe qui est associé à SSAC, SSAC63 a parlé de beaucoup de ces problèmes il y a de cela plusieurs années. Et un des points importants qui avaient été notés, c'était d'essayer d'en apprendre au maximum sur ce roulement de clés pour utiliser les données et l'expérience pour les autres roulements de clés. Donc c'est important.

Est-ce qu'il y a d'autres questions rapides pour Roy ? Je sais que le déjeûner nous attend. Robert, allez-y.

ROBERT MARTIN-LEGENE : Une chose que l'on pourrait prendre en compte pour ces roulements, ce serait d'avoir, je ne sais pas si vous êtes d'accord ou pensez que je suis fou, mais avoir les serveurs racine fournir des données à l'ancienne clé, et d'autres serveurs assignés à la nouvelle clé. Donc la nouvelle clé continuera de demander... Je ne sais pas, qu'est-ce qu'il va se passer à ce moment-là ? Est-ce qu'il va y avoir une panne de service pour les utilisateurs ? Mais on verrait qui utilise quelle clé, la nouvelle ou l'ancienne.

ROY ARENDS : Cette idée n'est pas mauvaise en elle-même. Elle a été mentionnée plusieurs fois. Le problème est le suivant. Vous avez

un ensemble de serveurs racine avec l'ancienne clé, l'autre avec la nouvelle clé, et vous devez observer cette progression naturelle de la configuration allant vers la nouvelle clé. C'est très difficile à mesurer. Cela n'aide en rien. Ce que nous devons faire, c'est passer à la clé 2017. Et la question qui va se poser, c'est quand est-ce qu'on va éteindre, arrêter l'ancienne clé. Donc on sait déjà où se trouve l'ancienne clé, si on a un bon échantillon. Donc je ne vois pas ce que cela apporterait. Je dirais non.

ROBERT MARTIN-LEGENE : Donc je ne pense pas que ce devrait être fait, mais ce pourrait être fait. Je ne crois pas que l'ICANN voudrait aller dans cette voie.

ROY ARENDS : Il y a beaucoup de choses qui pourraient être faites que l'ICANN ne veut pas faire.

RUSS MUNDY : Et bien nous allons pouvoir applaudir notre présentateur qui, pour la septième fois, a effectué cette présentation.

Et maintenant... Oui, Jacques ?

ORATEUR NON-IDENTIFIÉ : Il revient ; il est parti aux toilettes.

RUSS MUNDY : Ah.

Le quiz du DNS. Nous avons le temps de le faire.

ORATEUR NON-IDENTIFIÉ : Le déjeûner est à 12 :15, donc on a du temps.

GEOFF HUSTON : Donc la raison pour laquelle il n'y a pas de véritable réponse claire, c'est que lorsque vous avez deux clés listées sur le DNS qui sont signées avec l'ancienne clé, et bien cela, de manière implicite, vous permet de faire confiance aux matériaux signés avec la nouvelle clé parce que vous faites confiance à l'ancienne clé. Et même si vous allez sur un autre serveur racine, vous allez avoir une confiance, vous allez faire confiance à l'ancienne clé.

Et tout ce problème est compliqué par le fait que l'ancienne clé signe une nouvelle clé ; vous faites confiance à une ancienne clé tant qu'elle a été signée. Donc c'est difficile de séparer les deux clés sur la racine. C'est ça, le problème, de distinguer les noms de DNSSEC. Il y a des éléments qui peuvent être uniquement validés avec la nouvelle clé. Ce n'est pas toujours le cas, il y a des protocoles qui sont différents, il y a des résultats qui sont différents et cela, c'est est très difficile à effectuer. Je ne

suis pas sûr que les données seraient utiles à ce niveau parce que comme je l'ai dit auparavant, ce n'est pas les résolveurs qui posent problème. C'est les dégâts que vous allez faire aux utilisateurs, les problèmes que vous allez poser aux utilisateurs. Donc vous devez penser en ces termes. Et bien, vous vous concentrez sur l'utilisateur.

Jacques est rentré dans la salle, et je vais donc lui passer la parole.

JACQUES LATOUR : Donc d'autres questions ?

Je ne sais pas pourquoi on m'a demandé de poser ces questions pour le quiz, pour la petite interrogation.

Bienvenue donc à ces grandes questions sur le DNS à ICANN60. Vous avez devant vous le quiz avec dix questions. Donc vous avez cela devant vous. Sur la table à l'entrée, vous avez ces questions qui vous sont données, et tout le monde devrait avoir un stylo également. Voilà.

Alors les règles. J'ai appris ces règles de la part de Roy : j'ai toujours raison ; et même si j'ai tort, j'ai raison. C'est pour cela que je suis l'autorité ; je suis le maître de conférence. Une bonne réponse par question, un point par bonne réponse, dix questions, un maximum de dix points. Vous ne pouvez pas avoir

-17, -19. Vous voyez ? Maximum de dix points puisqu'il y a dix questions. Alors allons-y sans plus attendre.

Première question : à quelle date le roulement de la racine KSK était supposé survenir pour signer la zone racine ? A) le 11 octobre 2014 ; B) 11 octobre 2015 ; C) 11 octobre 2016 ; D) 11 octobre 2017 ; ou E) 11 octobre 2018. Et on a décidé de ne pas le faire l'année prochaine.

Alors trois, deux... zéro.

Deuxième question : quel feed de Tweeter suit les changements de la zone racine ? A) @therootchange ; B) @changeroot ; C) @diffroot ; D) @root ; et E) @IAmGroot.

Question numéro 3 : à quelle liste de publipostage devriez-vous vous abonner pour au mieux voir ou effectuer des rapports sur les problèmes concernant le DNS en général ? A) DNSoperation@list.DNS-OARC.net, vous avez toutes les adresses à l'écran : A), B) C), D), E). Et E) étant HelpWithDNS@ICANN.org.

Donc j'ai toujours raison. Alors je vais choisir la bonne réponse. C'était la troisième question. Nous passons à la quatrième.

Dans le draft IETF homenet.14, quel domaine est désigné pour utilisation non-unique pour les réseaux résidentiels et désigne ce domaine comme étant un domaine d'utilisation spécialisée ? Est-ce que c'est A) .home ; B) .rop.home ; C)

.home.mezo.kaza.mezo, en chinois ; D) home.rop, oui, je crois que c'est du chinois ; et E) .mezo ?

Question numéro 5 : quel ccTLD a été le plus récemment signé avec le DS dans la racine ? A) .ax pour les îles Åland ; B) .gw – c'est Guinée-Bissau ; C) .bm pour les Bermudes ; ou réponse D) .sa pour Saudi Arabia.

Trois, deux, un.

Ça, c'est très spécial. Désolé, je suis Canadien. On dit toujours désolé, mais qu'est-ce qui décrit le mieux les entités basées sur les DNS d'authentification des noms DANE avec la valeur numéro 2 des certificats TLSA ? A) sans affectation ; B) PKXDA-CA puis je plains les interprètes ; C) DANE-TA ; D) DANE-EE ; et E) PKIX-EE avec une contrainte sur les certificats de service. Donc voilà.

Question suivante, question 7 : quel pourcentage de tous les TLD dans la racine sont signés avec une délégation sécurisée de la DS dans la racine ? On en a parlé ce matin. Tout le monde dormait. J'en ai parlé ce matin. C'est important, je vous l'ai dit.

Alors c'est super. Question 8 : quel documents Paul Mockapetris a publié le 19 novembre marquant le début, le lancement du DNS ? C'est en novembre 1983. Alors est-ce que c'est BCP 16 et BCP 17 – c'est le A) ; B) BCP 42 et BCP 78 ; C) RFC 882 et RFC 883 ;

ou bien D) RFC 1034 et RFC 1035. Donc cela était une recherche Google.

Alors nous passons à la question numéro 9. Quelle est une méthode d'adressage de réseaux et de routage à laquelle les datagramme utilisent une route avec plusieurs nodes de destination sur la base des coûts étant moindres de la proximité avec un routage peu congestionné ? Est-ce que c'est A) Multicast ; B) Anycast, C) Unicast D : Subspacecast ; ou E) Flurrycast ?

Alors trois, deux, un, nous passons à la question numéro 10. Qu'est-ce que cela veut dire, DNS ? A) serveur de noms de domaine ; B) système de noms de domaine ; C) logiciel de noms de domaine ; D) service de noms de domaine ; ou E) espace de noms de domaine.

J'ai mis cette question ici parce que je ne sais même pas quelle est la réponse ; je ne suis pas sûr. De toute façon, je vais choisir la bonne réponse. Et après, on en parlera pendant le déjeûner. DNS... L'acronyme DNS.

Alors, vous passez à votre voisin votre document. Très facile, une réponse par question, un point par réponse, au maximum dix points, et on verra si je vais me tromper, n'est-ce pas ?

Question numéro 1, réponse D) : on devait le faire le 11 octobre 2017. C'est bon ? Il vous faut au moins un point pour aller manger. Je vous dis c'est la nouvelle règle. Si vous avez zéro, rien à manger.

Question numéro 2, la réponse est la réponse C) : @diffroot. Donc IAmGroot, je l'aimais bien.

Question numéro 3, réponse A) : DNS opération@list. C'est le bon endroit où il faut que vous envoyiez vos messages si vous avez des problèmes avec le DNS en général. Si vous n'êtes pas sur la liste, vous pourrez faire des recherches sur Google, rejoignez la liste, faites des recherches. C'est une bonne ressource. Je vous fais du marketing.

Question 4, réponse D) : .home. J'aime bien l'option C). Je pense qu'il faudrait que l'on ait un domaine long comme tout avec toutes les langues. Ce serait bien.

Question numéro 5, c'est le .gw, la Guinée-Bissau, qui a été ajoutée en 2017. Donc c'était la réponse B). C'était l'incorporation la plus récente.

Question numéro 6, réponse C) : DANE-TA. Vous avez bien répondu ? C'est pour vous que j'ai ajouté cette question. Alors c'est la Trust anchor assertion. C'est ça la bonne réponse.

Question numéro 7 c'était la réponse C) : entre 90 et 94 %. C'est 90 % des TLD qui sont signés.

Question numéro 8, réponse C) : RFC 882 et RFC 883 qui étaient écrites en 1983. Est-ce qu'il y a un rapport entre le 883 et 1983 ? Non ?

Question numéro 9, réponse B : Anycast. Et la nouvelle version pourrait être Subspacecast. Il faut qu'on commence à s'y mettre. Ou Flurrycast aussi, ce serait bien. On l'enverrait partout, cela fonctionnerait toujours. J'aime bien cela.

Question numéro 10 maintenant. Je ne savais pas très bien quelle était la réponse donc je me suis dit bon, pourquoi ne pas choisir le B).

Alors on va voir qui a gagné, qui est le gourou du DNS. Alors comptez les notes. Si vous avez cinq ou plus, levez la main. Six ou plus ? Sept ou plus ? Huit ou plus ? Neuf ou plus ? Et dix ? On est devant un grand gourou du DNS. Il faudrait qu'on ait un prix à vous remettre. Mais vous aurez le repas gratuit de toute façon. Ça, c'est le prix. Neuf sur dix ? Très bien, excellent.

JULIE HEDLUND : Alors, le déjeûner est prêt dans le hall 4. Si vous passez devant registration, l'enregistrement, il faut que vous preniez le couloir

de droite. Ce qu'il vous faudra sera le ticket. C'est tout ce qu'il vous faut.

[FIN DE LA TRANSCRIPTION]