ANDREA GLANDON : Bonjour et bonsoir à tous. Bienvenue à ce cinquième séminaire web de notre programme de formation de compétences d'At-Large 2018 concernant la première partie du roulement de la KSK, ce mercredi 13 juin 2018 à 21:00 UTC.

Nos présentateurs ce soir sont David Conrad et Andrei Kolesnikov.

Nous allons passer à l'appel étant donné qu'il s'agit d'un séminaire web. Nous avons des services d'interprétation en français et en espagnol. Je vous rappelle de bien vouloir dire vos noms au moment de prendre la parole pour que les interprètes puissent vous identifier sur l'autre canal linguistique et pour la transcription. Parlez également à un débit raisonnable afin de permettre aux interprètes de bien pouvoir interpréter ce que vous dites. Je rappelle à tous les participants connectés à travers le téléphone comme sur Adobe Connect de bien vouloir mettre en muet leur téléphone au moment de ne pas prendre la parole. Nous allons également mettre en muet toutes les lignes qui sont connectées à travers le téléphone pendant les présentations.

Merci de nous avoir rejoint. Je vais maintenant céder la parole à Tijani Ben Jemaa, président du groupe de travail de renforcement des capacités.

TIJANI BEN JEMAA : Merci Andrea. Bonjour et bonsoir à tous. Vous aurez remarqué qu'il s'agit de la première partie de notre séminaire web sur le roulement de la KSK parce que nous avons prévu de tenir deux séminaires web sur le

roulement de la KSK, dont l'un avant et l'autre suivant le roulement, s'il se fait, bien sûr.

Aujourd'hui, nous avons invité monsieur roulement, monsieur David Conrad, le CTO de l'ICANN responsable de la technologie de l'ICANN. Et c'est lui le responsable ultime du roulement. Étant donné qu'il s'agit qu'il s'agit de la personne qui connaît le mieux cette question, nous allons le consulter pour ce sujet.

Nous avons également un autre présentateur, monsieur Andrei Kolesnikov, l'agent de liaison de l'At-Large... Pardon. Andrei Kolesnikov est un membre du comité consultatif de la sécurité et de la stabilité.

ANDREA GLANDON : Tijani, êtes-vous toujours connecté ? On ne vous entend plus.

TIJANI BEN JEMAA : Oui, me voilà. Est-ce que vous m'entendez ?

ANDREA GLANDON : Oui, on vous entend maintenant, Tijani.

TIJANI BEN JEMAA : Très bien, parfait. Alors dans ce cas-là, nous allons commencer avec les présentations mais avant cela, Andrea a quelques annonces administratives à faire. Allez-y, Andrea.

ANDREA GLANDON : Oui, merci. Alors je ferai quelques annonces administratives avant de commencer.

Pour les questions et les réponses au cours de ce séminaire web, vous pouvez les envoyer à travers le chat qui se trouve dans le coin en bas à gauche sur votre écran. Vous pouvez également envoyer des commentaires à travers le chat au milieu de l'écran. Et tout cela sera envoyé aux présentateurs à la fin de la présentation. Remarquez pourtant que nous avons une séance de questions et réponses à la fin des présentations et une interrogation à la fin.

Pour ce qui correspond à l'interrogation, nous allons identifier les questions dans l'écran de la salle Adobe Connect. Donc soyez prêts à y répondre à travers l'outil de sondage.

Finalement, à la fin de notre séminaire web, après les questions et réponses, nous aurons un sondage d'expérience d'utilisateur qui comprendra six questions. Donc veuillez bien rester trois minutes à peu près pour bien vouloir les compléter. Il est important pour nous d'avoir vos retours concernant ce programme de renforcement des capacités d'At-Large. Merci.

Tijani, je vous redonne la parole.

TIJANI BEN JEMAA : Merci Andrea. Nous allons maintenant céder la parole aux présentateurs. Qui va commencer ? Est-ce Andrei ?

DAVID CONRAD : En fait, nous avons décidé que je présente justement la présentation et que par la suite, je cède la parole à Andrei et que nous puissions par la suite passer aux questions et réponses, si cela vous convient. Est-ce correct ?

TIJANI BEN JEMAA : Oui, tout à fait.

DAVID CONRAD : Très bien. À ce moment-là, je commence. Il semblerait que j'aie pris le contrôle de la salle. Je suis David Conrad, le responsable technologie de l'ICANN et je viens vous parler aujourd'hui sur le roulement de la clé de signature de clé du DNSSEC.

Pour commencer, je présenterai quelques connaissances de base. Il s'agit d'une présentation liée au système des noms de domaine et en particulier, aux extensions de sécurité qu'on y apportées.

Lorsqu'on a créé le système des noms de domaine, il y avait un bug structurel qui permettait, au moins dans la théorie, aux pirates de répondre à des requêtes et que ces réponses soient acceptées par le système, ce qui permettait à la cache d'être empoisonnée, ce qui faisait que l'on avait des problèmes de cache et de résolveurs et que l'on puisse avoir des attaques de l'intermédiaire par exemple ou d'autres types d'attaque. Mais ces formes d'attaque, en général, ne sont pas fréquentes parce qu'il y a des manières beaucoup plus simples d'attaquer l'infrastructure. Or, dans la théorie, ce sont des attaques théoriques qui ont été démontrées dans la pratique.

Mon avis personnel est que vu que les attaques les plus simples se compliquent à travers les nouvelles infrastructures, à travers les applications fixes, à travers les mots de passe plus forts, nous commençons à avoir une augmentation du niveau des attaques qui ne peuvent pas être empêchées par le DNSSEC. Un de ces types d'attaques était récemment mis en œuvre contre myetherwallet.com par exemple et cette attaque en particulier aurait pu être empêchée par le DNS.

Donc le DNSSEC est un ensemble d'extensions de sécurité qui ont été définies pour adresser ce bug en particulier à travers la spécification du protocole du DNS. Et les extensions, donc, appliquent des signatures numériques aux données numériques suivant la hiérarchie qui est inhérente au DNS pour pouvoir atteindre une échelle de masse. Et dans la racine ainsi que dans d'autres zones, bien sûr – mais nous parlons ici de la racine –, il y a des règles qui ont été divisées. Donc on a divisé les rôles. On a la clé de signature de clé qui signe en ensemble d'autres clés et la clé de signature de zone qui signe les données de zone. Cette division en particulier a été faite pour permettre que l'on modifie fréquemment les clés de signature de zone afin de pouvoir modifier les clés de signature de clé. Cela sera expliqué un peu plus tard.

Le DNSSEC est composé de deux parties, à savoir la signature de la zone qui est faite par les administrateurs de la zone, c'est-à-dire les administrateurs de TLD et des espaces de nouveaux gTLD, qui ont l'obligation contractuelle de signer leur zone à l'aide du DNSSEC. Il y a également beaucoup de ccTLD qui signent également leur zone. La racine à l'origine était signée à partir de 2010 et la structure est de signer les données de zone, compléter le [hash] avec [inintelligibles]

pour garantir que ces données de zone, si elles étaient modifiées une fois qu'elles ont été signées, que l'on puisse détecter cette modification.

Cette identification de la modification est appelée validation, qui est faite par les résolveurs récursifs. Et au moins dans la théorie, les résolveurs minimum peuvent également vérifier les signatures. Les résolveurs minimum sont les logiciels qui sont liés aux applications qui sont utilisées. Le résultat conséquent est que la validation avance et à ce moment-là, la réponse est envoyée comme validation. Si la validation n'est pas approuvée, on obtient un message d'erreur. Mais le DNSSEC n'empêche pas les modifications des données de zone par les attaquants. Pourtant, cela nous permet d'identifier ces modifications lorsqu'elles y sont apportées.

Le DNSSEC de la zone racine et la clé de signature de clé sont au premier niveau dans la hiérarchie de cette chaîne d'informations, qui permet que les informations soient validées. La validation se fait utilisant des données du DNSSEC qui ont une signature, le validateur vérifie la signature, vérifie qu'elle corresponde à la signature du parent. Si c'est validé, cela suit au niveau suivant, et ainsi de suite, jusqu'à la racine. À la racine, étant donné qu'il n'y a plus de zone supérieure ou parent qui permet d'identifier les informations pertinentes pour voir s'il y a eu des modifications, il y a, sur chaque résolveur qui a la validation de DNSSEC habilité, une ancre de confiance. Cette ancre de confiance est la partie publique de la clé de signature de clé en elle-même.

Le DNSSEC utilise une cryptographie asymétrique, c'est-à-dire qu'il y a des clés publiques et des clés privées. Les clés publiques font partie de la racine et sont configurées dans les résolveurs.

Qu'est-ce que cela veut dire ? C'est-à-dire si l'on veut modifier la KSK de la zone racine, on génère une nouvelle clé privée et une nouvelle clé publique. On a une nouvelle paire de clés et on devra changer la configuration de tous les résolveurs dans le monde pour refléter la nouvelle portion de la clé publique.

Historiquement, on a toujours eu une clé qui était générée lorsqu'on signait la racine à partir de juillet 2010, que l'on connaît comme la KSK 2010. Or, nous avons créé une nouvelle KSK en 2017 qui sera opérationnelle à un moment donné cette année, ce que nous appelons la KSK de 2017.

L'impact de cela implique que les opérateurs des résolveurs récursifs, en général des fournisseur de services internet ou des opérateurs de réseau d'entreprise, bien que tout le monde pourrait opérer son propre résolveur, peuvent soit vérifier sa configuration pour voir si le DNSSEC est habilité d'une part et d'autre part, si la configuration et les informations de configuration contiennent la KSK de 2017 et la KSK de 2010 ou alors, s'il n'ont que la KSK de 2010 dans leur configuration de base. S'ils n'ont que la KSK de 2010, cela indique un problème.

La KSK 2010 est celle qui est utilisée à l'heure actuelle. Il n'y avait rien d'autre avant. C'est la partie publique qui est configurée dans les résolveurs. Et si vous avez habilité la validation, cette clé sera la clé qui est utilisée pour valider les données.

Si vous avez habilité le DNSSEC – et la plupart des résolveurs de validation le font d'ailleurs –, il y aura un système automatisé pour mettre à jour cette clé et il y a quelques mois, je ne sais plus à quelle date, la nouvelle clé, la KSK de 2017, a été insérée automatiquement

dans ces données de configuration. Et 2017, ce n'est pas une erreur de frappe ; cette clé a été générée en 2017 et on avait prévu qu'on pourrait probablement pouvoir le mettre en œuvre en 2017. Mais comme on vous expliquera par la suite, ce roulement a été mis en suspend pour faire quelques recherches et quelques enquêtes. On compte avancer mais cela n'a pas été fait pour l'instant. Donc voilà mon explication potentielle sur pourquoi vous pourrez avoir mal compris de quoi il s'agit.

Le roulement de la KSK est apparu comme un résultat de la planification qui a commencé en 2013. Et lorsque nous avons signé la racine en 2010, dans la déclaration de la pratique du DNSSEC qui est un document de politique qui accompagne le DNSSEC au moment de signer la racine, nous avions promis de modifier la KSK après une période de cinq ans. Donc on a commencé avec ce processus pour penser à la planification d'une modification en 2013. Et puis, il y a eu une annonce qui nous a un peu distrait, qui était le transfert de la supervision des fonctions IANA. Donc la planification a été mise en suspend parce qu'on ne voulait pas tout modifier en même temps dans le cadre, bien sûr, de cette transition de l'IANA. On avait déjà pas mal de pain sur la planche à ce moment-là. Et au moment auquel la transition de l'IANA a commencé à avancer sans avoir besoin de vérifier les aspects techniques de cette transition, nous avons initié la planification et nous avons conçu tout le plan en 2015.

Or vu la manière dont laquelle le roulement automatisé fonctionne, nous avons dû adopter une approche plutôt lente et nous avons travaillé sur le cycle de mise à jour associé à la KSK normal, c'est-à-dire que nous avons commencé à travailler dans les différentes installations

pour pouvoir signer les différentes KSK ; cela se fait une fois par trimestre. C'est-à-dire que toutes les mesures qui devaient être prises pour le roulement de la KSK se sont faites de manière trimestrielle, comme d'habitude. C'est la norme définie dans le RFC 5011 et c'est le document à travers lequel nous supposons que tous les résolveurs mettrons à jour leur clé.

Dans la pratique, ce n'est pas toujours le cas. Il y a des personnes qui ne mettent pas à jour de manière automatique leur KSK pour différentes raisons, à savoir parce que l'on pourrait avoir des problèmes provoqués lorsque ces clés sont modifiées à distance. Mais sachant que le protocole a été défini, on a décidé de l'utiliser comme une règle pour l'application de la signature elle-même.

Le jalon important ici – c'était le plan original – était de déployer la KSK en octobre 2016. À l'époque, nous étions qualifiés. Nous avions fait une qualification, c'est-à-dire que nous avions le local de gestion de clé qui se trouve aux États-Unis. Nous avions un deuxième local, donc l'un sur la côte Est, l'autre sur la côte Ouest aux États-Unis. Nous avions donc ces deux endroits. Nous avions donc les modules de sécurité qui nous permettaient d'avoir un très haut niveau de sécurité.

Et par conséquent, en février 2017, la nouvelle clé KSK 2017 était prête à être utilisée. Après le 2 février, nous sommes commencé à publier cela et cela a été fait de différentes façons. Nous avons fait cela à travers des T-shirts, sur le site internet de l'IANA, etc. Et en juillet 2017, le processus 5011 a commencé et la mise à jour a commencé à avoir lieu, ce qui voulait dire que la nouvelle KSK a commencé a être insérée dans les

résolveurs qui étaient configurés pour accepter cette mise à jour automatisée.

Le plan était que le 11 octobre 2017, nous allions pouvoir commencer à utiliser la nouvelle KSK en signant avec la clé de signature de zone, qui aurait dû être faite. Ensuite, nous avons discuté de ce point-là et nous avons décidé de reporter cela parce que nous voulions savoir exactement ce qui se passait. Donc le plan a été d'annuler la clé antérieure qui ne sera pas utilisée dans le futur. Et nous n'avons pas encore décidé exactement ce que nous allons faire. Nous allons donc annuler cette clé dans le processus automatisé qui va permettre de travailler et de mettre à jour les nouvelles clés et la configuration des résolveurs.

Mais comme tout le monde le sait, nous avons suspendu le roulement de KSK parce que nous avons commencé un processus pour reprendre ce roulement de clé. Et actuellement, un an après le plan qui était à l'origine d'utiliser la nouvelle KSK et de la mettre en place le 11 octobre 2018, nous pensons que le 11 octobre 2018, nous allons pouvoir utiliser cette nouvelle clé. L'annulation de la KSK 2010 aura lieu un trimestre plus tard, un trimestre après. Nous allons supprimer cette clé mais nous ne voulons pas nous presser. Nous voulons prendre notre temps pour être sûrs de ne pas commettre d'erreur.

Alors pourquoi est-ce que nous mettons à jour ces dates [inintelligible] ? Lorsque nous avons commencé ce processus de roulement, il n'y avait pas de moyen de mesurer les configurations des résolveurs. Nous travaillions vraiment dans l'obscurité, nous n'avions pas idée du nombre de personnes qui utilisaient ce système. Et le RFC a voulu faire une mise

à jour. Et nous nous sommes basés sur un plan de communication pour s'assurer que tout le monde faisait la mise à jour de manière appropriée.

Cependant, pendant le projet de roulement de KSK, à cette époque-là, on a créé un RFC qui définit un mécanisme pour permettre de mesurer la façon dont les résolveurs étaient configurés pour être publiés. Et les résultats de cela ont été très surprenants. Les spécifications pour ces technologies et 8145 ont été présentées en avril 2017. Et en août 2017, un auteur de ces recherches a décidé de travailler avec Verisign, qui opérait deux serveurs racine à l'époque, et ils ont voulu voir s'ils voyaient des signaux venant de ces publications, de ces mécanismes de mesure de publications. Et on a vu des données et cela nous a vraiment étonné, ces données qu'on a constatées qui existaient et qui nous ont même inquiétés, je dirais. Et c'est là que nous avons décidé de reporter le roulement de KSK, parce qu'on voulait comprendre d'abord ce qui se passait.

Donc j'ai mentionné le RFC 8145. Il s'agissait donc des connaissances de l'ancre de confiance. Ah, il y a un petit problème ici sur Adobe Connect. Je vais vous montrer ce tableau qui montre le pourcentage des résolveurs qui annonçaient le KSK 2010. Je vais vous envoyer une URL pour que vous puissiez voir les statistiques en temps réel de ces résultats de cette publication du KSK 2010 et KSK 2017. Et Adobe ne me le permet pas de le faire, donc je ne peux pas vous montrer cela sur le PDF comme c'était prévu, mais peu importe.

Nous avons vu en septembre 2017 – donc un mois avant la date à laquelle nous avions prévu d'utiliser la nouvelle clé –, nous avons

constaté donc qu'il y avait un nombre très élevé de résolveurs qui disaient qu'ils avaient seulement la KSK 2010 et qui n'avaient pas actualisé leur KSK 2017. Et à ce moment-là, nous avons pensé que le pourcentage serait en-dessous de 1 % et nous avons constaté que ce pourcentage était de 7 % selon Verisign. Par conséquent, ICANN a commencé à regarder les données de serveurs racine auxquelles nous avions accès. Et nous avons essayé d'obtenir aussi des données de différents serveurs racine de Californie et autres. Et nous avons commencé à obtenir des données, à les analyser et les résultats étaient presque pires que ce que Verisign avait annoncé. Donc c'était vraiment étonnant. Et un problème, le pourcentage de résolveurs qui montrait qu'ils n'avaient que la KSK 2010 augmentait, à tel point que le code 8145 semblait, donc, ne pas être utilisé.

Lorsque nous avons commencé à regarder ces résultats, nous avons des questions que nous nous posions. Que nous disaient les données ? Il s'agissait d'un code qui mettait en œuvre quelque chose qui n'existait pas jusqu'au mois d'avril 2017. C'était tout à fait nouveau et cela aurait dû fonctionner avec des résolveurs qui auraient dû utiliser cela seulement. Et les gens auraient dû mettre en œuvre ce système dès le début. Les développeurs de résolveurs auraient dû utiliser ce système.

Donc on ne comprenait pas ce s'est passé. On a essayé de chercher les codes qui existaient dans le système du DNS et nous avons constaté une série de bugs dans plusieurs résolveurs assez populaires. Mais cela ne suffisait pas à expliquer ce qui se passait.

Donc nous avons commencé à analyser les informations que nous avions au niveau du serveur racine. Nous avons essayé de faire un suivi

des personnes qui généraient ces annonces que nous recevions qui nous montraient que seulement la KSK 2010 était configurée au niveau du serveur racine. Nous avons vu que les adresses IP des résolveurs étaient en train de faire des requêtes aux résolveurs. Et là, le modèle le plus simple que l'on pourrait avoir pour voir comment fonctionne le DNS, si on a un plan qui appelle le résolveur qui à ce moment-là appelle la racine, il y a toute une série de systèmes qui permettent de retransmettre, de faire suivre les requêtes de façon à ce que les adresses IP que nous recevons du résolveur n'ont pas de relation avec le résolveur qui l'a générée en réalité. Donc on a une chaîne d'appareils. Donc on a cette chaîne et on a peu d'informations nous permettant de trouver la source de ces informations, le résolveur qui est à l'origine de cela.

Donc nous avons demandé à une série de personnes de travailler là-dessus, d'essayer de comprendre quelles étaient les causes de tout cela. Et on a des machines virtuelles qui sont configurées comme cela. Les gens ont commencé à faire les tests. Et puis il y a une série de logiciels qui ont commencé à être utilisés dans ce sens, qui avait seulement la KSK 2010 et qui ont interagi avec les résolveurs. Et les machines ont commencé à n'envoyer que les annonces de KSK 2010. Et on ne comprenait pas vraiment ce qui se passait.

On a continué à faire des recherches là-dessus et comme cela a été dit, en 2017, nous avons constaté qu'il n'y avait pas vraiment une faille dans le plan de projet ou dans son exécution, parce que notre plan anticipait ce type de problèmes, ces problèmes de ce type. Il y avait tout un plan en cas de panne qui était prévu, de façon à pouvoir réagir en cas d'imprévus. Et tout s'est assez bien passé. Mais comme on essayait de

comprendre ce qui se passait, qu'on avait du mal à comprendre ce qui se passait, on a fait ce que les organisations font dans ces cas-là, donc lorsqu'elles ne comprennent pas ce qui se passe, donc nous avons demandé à la communauté de nous aider et nous avons fait participer des experts en DNSSEC pour essayer de trouver et d'identifier une manière d'avancer. Nous avons préparé un plan mis à jour, nous l'avons présenté aux commentaires publics, nous avons obtenu une série de commentaires et ceux d'ALAC aussi ont été reçus. Et finalement, nous avons obtenu un plan révisé. La réponse courte par rapport à ce plan serait que les données de 8145 n'était pas exactes parce qu'elles ne reflétaient pas choses telles qu'elles se passaient. On avait des résolveurs qui étaient configurés, mais on ne savait pas combien d'appareils étaient derrière ces résolveurs. Donc les utilisateurs ici étaient concernés puisque si le système de KSK 2017 était déployé, on avait peut-être 25 % des requêtes de DNS qui devaient être invalidées parce qu'on allait avoir un petit ou un grand nombre de résolveurs, on ne savait pas, Google ou d'autres résolveurs, des commissaires de services aux États-Unis par exemple qui n'allaient pas fonctionner correctement. Ce qui voulait dire que l'annonce du résolveur 8145 pouvait initier un résolveur qui allait paraître mal configuré et qui allait peut-être ne pas fonctionner correctement. On a fait des tests et on avait l'impression qu'il y avait deux possibilités : ou les utilisateurs n'avaient aucun impact, ou bien cela ne marchait pas.

Ici, dans cette discussion, comme nous ne savons pas vraiment quelles sont les données qui sont reflétées réellement au niveau de l'impact sur les utilisateurs, on ne pouvait pas compter sur ces données puisqu'il y avait des outils dans ce sens.

Donc ici, vous voyez le rapport d'ancre de confiance pour tous les serveurs racine. Vous voyez qu'il y a un pic ici qui nous montre 180 000 adresses IP uniques. Cela indique donc... je pense qu'il y a un problème de nouveau... donc 180 000 annonces que l'on pouvait voir. Donc on a enregistré ici en rouge le KSK 2010.

Et vous voyez sur ce graphique, ici, vous voyez les pourcentages. Ces diapositives ont été faites pour une présentation pour une recherche. Donc ici, la réalité en tout cas, c'est que si la KSK est mal configurée et si nous avançons et si nous signons la racine avec la KSK 2017, cela va vouloir dire que toutes les résolutions des résolveurs vont être défaillantes, elles vont avoir des failles seulement parce que la clé est roulée.

Donc nous devons maintenant revenir à la communauté et essayer de communiquer de la meilleure manière possible. Et la réalité actuelle, c'est que nous n'allons pas pouvoir inclure tout le monde. Et la communauté, lorsqu'elle a mis en place ce plan de roulement de clé, a compris cela et elle a mis des critères. Si moins de 1 % des utilisateurs finaux vont avoir un impact négatif à cause de ce roulement, ce sera un succès et on ne reviendra pas en arrière dans le roulement de clé.

Les informations que nous avons reçues, c'est qu'une série de résolveurs étaient mal configurés mais cela ne nous dit pas combien d'utilisateurs finaux allaient recevoir un impact négatif de cela. Donc nous avons demandé sa contribution à la communauté et la communauté nous a dit : « On n'a pas d'informations sur les utilisateurs finaux. On sait que les résolveurs en grande mesure sont bien configurés. » Et peut-être qu'il faut continuer à aller de l'avant et voir

un petit peu ce qui se passe, en espérant qu'on aura moins de 1 % impactés, qui n'ont pas le système correctement installé.

Comment reconnaître cette KSK 2017 ? Alors vous avez le numéro 20326 ; cette étiquette de la clé de la KSK 2017 devrait apparaître dans votre configuration. Ensuite, l'enregistrement de ressources DNS key est assez long, vous le voyez ici, c'est ce que la cryptographie fait, ce que cela provoque.

Bien. Maintenant, quel est l'état actuel du système ? Je dirais que la KSK a été modifiée dans de bonnes conditions. L'approche que nous avons est une approche prudente. Et les mises à jour automatisées et le système fonctionnent sur 30 jours. Nous avons déjà dépassé ces 30 jours, donc je pense qu'au mois d'août 2017, déjà, le système qui faisait la configuration automatisée était déjà réglé pour que la KSK 2017 puisse être déployée. Et on aurait pu à ce moment-là continuer mais vous le savez, nous n'avons pas pu, nous avons décidé de ne pas le faire. Voilà.

Donc le processus déploiement, du point de vue du validateur, il assume que le résolveur est configuré avec le DNSSEC est qu'il est configuré pour fonctionner. Tout le monde devrait avoir la nouvelle KSK. Si ce n'est pas le cas, vous devez l'ajouter manuellement si cela n'a pas été fait de manière automatique.

Alors comment est-ce qu'on sait que le résolveur a fait cette validation ? Vous pouvez envoyer une demande à dnssec-failed.org et si vous recevez une erreur « serve fail », cela veut dire que le DNSSEC est déployé. Si vous ne recevez pas cette réponse, cela veut dire que cette validation du DNSSEC n'existe pas. Si vous avez accès sur un système

unique, vous devez trouver quelque chose de ce genre. Il y quelque chose qui va vous permettre d'envoyer une demande et l'adresse IP ou le noms de domaine du résolveur que vous voulez [inintelligible] envoyer ici et on va vous envoyer une réponse. Si on vous dit « serve fail », cela veut dire que la validation du DNSSEC est activée et cela est une indication que la validation n'est pas activée, sur l'autre diapositive.

Alors on nous demande souvent comment est-ce que je peux dire si la KSK 2017 a été configurée correctement sur mon résolveur. Hélas, la réponse est qu'on ne peut pas le dire, c'est difficile à dire. Il n'y a aucune manière d'avoir accès au résolveur au niveau de la gestion, pour être capable de savoir si la KSK a été correctement configurée. Cela est une nouvelle spécification qui s'appelle sentinelle KSK, qui permet d'envoyer une requête pour demander des informations sur quelle KSK est dans votre résolveur. Cela va prendre un certain temps.

Si vous avez accès à un niveau ou un autre du résolveur, vous pouvez vérifier avec quelques commandes si la KSK fonctionne, quelle est votre KSK et cela va vous donner toutes les informations concernant les différentes approches que vous pouvez utiliser. Pourtant, à l'heure actuelle, pour la plupart des personnes et pour les utilisateurs, il n'est pas possible de voir quel est le résolveur configuré pour la KSK et ce n'était donc pas la manière dont on a conçu le DNS.

Cette URL que vous avez à l'écran fournit certaines informations concernant les ancres de confiance, pour vérifier quelles sont vos ancres actuelles, mais c'est au niveau du gestionnaire, pas au niveau des utilisateurs finaux que cela est disponible.

Si vous avez la bonne configuration en ce moment, vous devriez avoir deux ancres de confiance : la KSK 2017 avec l'identificateur de clé 20326 et la clé 2010 qui a l'identificateur 19036. Comme on l'a dit, la KSK 2010 sera supprimée une fois qu'on aura migré complètement à la KSK 2017. On n'a pas une date exacte en ce moment mais ce sera à un certain moment dans l'avenir.

Comment ces informations seront-elles visualisées ? Vous avez ici quelques informations que je présenterai rapidement, qui montrent les différentes manières de voir la KSK. Donc c'est facile à voir, comme vous voyez, sur bind ; sur unbound, c'est un peu plus compliqué. Vous avez ici la réponse pour voir quelle est la KSK qui est configurée [inintelligible]. Mais pourtant, il est toujours possible d'avoir ces informations. Si vous avez les deux KSK installées, vous n'avez rien à vous en soucier, c'est-à-dire que tout fonctionne correctement. Autrement, il faut régler vos paramètres accédant à ce site web où vous avez les différentes versions des résolveurs et on vous explique comment... Une fois que vous aurez la KSK officielle disponible à travers un fichier de DNS sur notre site avec un fichier XML qui contient les mêmes informations qu'un registre DNS et il y a également d'autres informations, d'autres fichiers qui sont un peu plus communs. Donc en fait, la mise à jour du logiciel vous donnera des informations de configurations mises à jour qui comprendront les bonnes informations.

Pour ce qui est de l'ancre de confiance, si vous n'avez pas la bonne clé, que vous avez utilisé la nouvelle clé pour la zone racine, ce que vous verrez est une erreur de serveur, vous aurez un message d'erreur pour toutes les requêtes que vous enverrez. Si vous avez accès au fichier de registre de l'hôte, vous verrez ce qui se passe. Mais en termes généraux,

si vous êtes un utilisateur final, vous vous rendrez compte du fait que vous ne pourrez pas faire des recherches. Cela en soi vous indiquera que la KSK n'a pas été mise à jour.

Alors prochaines étapes, nous allons révoquer la KSK 2010 à un moment ou à un autre une fois qu'on aura utilisé la KSK 2017 pour signer toutes les clés de signature de clé. À moins que la communauté nous indique autrement, il y aura plus de roulements de la KSK. Comme on l'a dit, il y avait une déclaration de pratique du DNSSEC qui indiquait que la KSK était modifiée tous les cinq ans. Donc l'idée sera de continuer à rouler de nouvelles clés tous les cinq ans. On espère pouvoir respecter cela et c'est le plan, à moins que la communauté nous indique autrement. On nous a même suggéré d'accélérer la fréquence de roulement de nouvelle KSK pour garantir que l'infrastructure de KSK existe pour nous permette de mettre à jour la KSK si besoin, ce que nous exerçons constamment, croyant que si on ne fait pas quelque chose au moment où cela est nécessaire, cela ne sera plus disponible lorsqu'on en aura besoin. Il y en a d'autres qui ont dit que tout ce roulement de la KSK n'était pas une bonne idée, que cela devrait être la dernière fois qu'on le fait. Mais à l'heure actuelle en tout cas, on est convaincu que la bonne fréquence pour la mise à jour est tous les cinq ans. Donc après le 11 octobre 2018, nous recommencerons à zéro avec le roulement d'une nouvelle clé et cette clé sera active jusqu'en 2023.

Quelques fichiers ressources mises à disposition par l'ICANN. Vous voyez ici qu'il y a un nombre d'outils disponibles pour valider l'ancre de confiance, pour vérifier le résolveur, des sites d'informations pour expliquer le roulement de la KSK, son importance, etc.

On a également un site pour l'ancre de confiance que vous pouvez utiliser dans votre système automatisé pour mettre à jour les logiciels de manière périodique pour vérifier et modifier la KSK si besoin.

Nous avons également un test de mise à jour pour permettre aux personnes qui utilisent un système automatisé de vérifier que tout fonctionne correctement. Cela continue de fonctionner. Si vous accédez à ce site web, cela vous expliquera comment accéder à ce système de tests, qui est valable pour tous ceux qui opèrent ces résolveurs automatisés qui ont allumé le support technique du RFC 5011.

Les informations liées au roulement de la KSK de l'ICANN sont disponibles sur la page sous quick links, donc les liens que vous avez ici.

Et encore une fois, en ce concernant les URL que vous pourrez trouver utiles ou peut-être pas, vous avez ici toutes les informations.

Cela dit, je vais maintenant céder la parole à Andrei, qui nous parlera de la gestion de la KSK au niveau des ccTLD. Andrei, allez-y.

ANDREI KOLESNIKOV : Merci David. Pour commencer, je voudrais dire que je me sens très rassuré du fait d'avoir toutes ces informations à l'écran et que j'espère que l'ICANN fasse un bon travail de sensibilisation pour que ce message puisse être transmis à tous les gens qui utilisent ces résolveurs et qui ont besoin de ces résolveurs. Je serai un peu pratique et je répéterai quelques aspects que vous avez abordés.

Donc pour rappel, le DNS est un système [distribué] qui commence à un point. Donc avec un point, on commence déjà à signer la zone racine et

tous les TLD suivent les mêmes formats, c'est-à-dire que le DNSSEC utilise une cryptographie de base, nous avons une clé secrète qui est vérifiée avec la clé publique, c'est-à-dire qu'il y a deux clés, la clé privée et la clé publique. L'une est la clé de signature de zone, l'autre est la clé de signature de clé. Il semblerait que c'est une question de magie, mais que je sache, la cérémonie qui a eu lieu pour la signature des clés montre... Lorsque l'on signe la zone, il y a également une présentation de représentants auxquels la communauté fait confiance. C'est eux qui viennent vérifier la cérémonie, qui voient que tout se déroule correctement et qu'ils vérifient les aspects importants pour la communauté.

Donc dans le cas des TLD, ce sont les fonctionnaires qui entretiennent les clés [publiques] qui font partie de la KSK. Mais si vous passez au niveau suivant du TLD, vous voyez – c'est ce qu'on avait fait en 2012 – que la clé est signée avec des noms de domaine. Et cela se fait sans connectivité internet sur un ordinateur qui est connecté au modèle de matériel sécurisé. Donc cela implique une clé qui est téléchargée dans votre résolveur de la zone. Après, cette clé est déployée dans l'ancre de confiance et cela veut dire que tout le système fonctionne suivant le principe que les noms de domaine font confiance à la zone, qui fait confiance aux TLD également. Donc c'est cela le principe. On ne peut pas éliminer un acteur de ce schéma. Donc beaucoup de ccTLD exploitent leur TLD suivant les registres de DNSSEC. Beaucoup de signatures qui sont dans la zone dans cet entourage sont utilisées pour maintenir ce système de confiance. C'est pour cela que la signature de la clé dépend des résolveurs qui utilisent ces ancres de confiance.

Nous avons ce soir parmi nous l'un des plus grands experts en matière de DNSSEC, Russ Mundy, qui l'une des personnes qui comprennent véritablement tous les détails du DNSSEC. Je n'ai pas de présentation ici, mais je suis du SSAC et j'appartiens également à l'ALAC. Donc l'idée était de fournir autant d'informations que possible sur le DNSSEC aux gens de l'ALAC et d'At-Large parce qu'avec la KSK dans le processus, il est important de comprendre quels pourraient être les problèmes techniques associés aux versions de logiciels qui ont été divulguées en 2010. Donc il est important pour comprendre comment tout le système du DNSSEC fonctionne et c'est pour cela, j'imagine, que Tijani a proposé de faire ce séminaire web.

Ma présentation était très courte, j'en suis déjà à la fin. Si quelqu'un veut savoir comment signer ce TLD de zone, vous pouvez me contacter séparément et je vous expliquerai en plus de détails le fonctionnement.

Tijani, je pense qu'on en est au moment des questions et réponses, n'est-ce pas ? Allô ?

ANDREA GLANDON : Tijani ?

DAVID CONRAD : Il paraît qu'il est en muet.

ANDREI KOLESNIKOV : Bien. Vu qu'on a Russ parmi nous, je pense qu'on pourrait peut-être essayer de répondre aux questions des participants à ce séminaire web.

ANDREA GLANDON : Est-ce que vous voulez que l'on passe à l'interrogation d'abord ?

DAVID CONRAD : On a d'abord quelques mains levées. Donc peut-être qu'on pourrait répondre aux questions avant l'interrogation ?

ANDREA GLANDON : Oui, bien sûr.

DAVID CONRAD : Je donnerai la parole à Alan qui semblerait être le premier à avoir levé la main.

ALAN GREENBERG : Merci. Vous avez expliqué les critères que vous avez pu utilisés ou que vous pourriez toujours utiliser pour revenir en arrière avec le roulement de la KSK. Donc qu'entendez-vous par « revenir en arrière », « rouler en arrière » ? Est-ce que cela est possible et quels sont les détails ?

DAVID CONRAD : Le plan initial de la communauté comprenait des critères disant qu'on aurait pu revenir à la KSK de 2010 si plus de 0,1 % des utilisateurs finaux avaient un impact final de ce roulement. Les critères qui avaient été définis par la communauté ne comprenaient pas très bien ce que cela impliquait parce que nous n'avons pas de moyens faciles pour savoir comment les utilisateurs finaux sont touchés par ce roulement.

En ce moment, on est en train de normaliser tout cela avec l'IETF et cela sera mis en œuvre avec quelques résolveurs suivant les normes existantes. Et ce sera mis en œuvre par un troisième résolveur. Mais une fois que cela sera fait, il y aura plus de personnes qui pourront le modifier, il y aura plus de temps avant que cela soit déployé. Une fois que cela sera déployé, on pourra avoir une idée un peu plus claire de la quantité d'utilisateurs finaux qui sont touchés par cette nouvelle KSK. Et à ce moment-là, on pourra savoir un peu mieux combien de personnes sont impactées par la KSK, si c'était un échec, combien serait affectées par cet échec.

Ce roulement en arrière impliquait que l'on cesse d'utiliser la KSK 2017 pour signer la racine et que l'on revienne à la KSK 2010 pour signer la racine.

Dans la théorie, cela voudrait dire qu'il y aurait une ou deux zones qui nous permettent d'identifier s'il y avait un problème si on revient en arrière. Et vu que ces clés sont censées exister et mais que la mauvaise configuration n'aurait un impact que sur l'ancienne clé, on reviendrait à l'utilisation de l'ancienne clé pour signer la zone racine, ce qui serait direct et assez simple, sans trop d'impact. Mais malheureusement, vu la manière dont le DNS fonctionne avec le cache et tout cela, il y aurait sans doute une grande quantité de bouleversements. Donc on préfèrerait essayer d'éviter de rouler en arrière cette nouvelle KSK. C'est pourquoi on a décidé de mettre en suspend le roulement jusqu'à ce que l'on aurait mieux compris ce qui se passait, quelles étaient les données qu'on avait.

Or, cela n'apparaît pas dans des diapositives mais une de nos analyses que nous avons faites avec les gens d'APNIC était de corréler les annonces de 8145 qui apparaissent dans les serveurs racines et les données, les serveurs d'APNIC à travers Google Ads et à travers des requêtes qui utilisent le DNSSEC dans les navigateurs. Et les informations que nous avons obtenues à travers cette approche sont plus rassurantes dans le sens que les chiffres que nous avons établis sembleraient être de moins de 0,05 % de résolveurs au niveau des résolveurs qui sont mal configurés. Donc les utilisateurs finaux seraient 0,05 % à avoir un impact, donc on est à moins de la quantité qui lancerait un roulement en arrière.

ALAN GREENBERG : Bien, merci. Donc pour résumer, le roulement en arrière du roulement, conceptuellement, est comme si on éteignait la lumière et puis il pourrait y avoir des problèmes de cache pendant quelques heures ou pendant quelques jours, même. Mais ce serait assez rapide, outre les caches à long terme.

DAVID CONRAD : Oui. Il y aura une publication de la zone qui a été signée avec le KSK 2010 au lieu de 2017.

ALAN GREENBERG : La deuxième question. Je présume que le seul impact... Disons que l'annulation de la KSK 2010 trois mois plus tard signifie qu'on ne peut pas revenir en arrière. Est-ce qu'il y aurait une autre implication ? C'est la seule ?

DAVID CONRAD : Oui, c'est la seule.

ALAN GREENBERG : Bien, parfait.

DAVID CONRAD : Et je devrais dire que je me trompe peut-être ; Russ, dites-moi si je me trompe.

RUSS MUNDY : Je voudrais ajouter qu'il y a une question d'impact sur les utilisateurs finaux ici. Et presque tous les utilisateurs finaux ont à leur disposition deux ou trois, parfois quatre résolveurs du DNS. Et si un de ces résolveurs fonctionne correctement, ils auront peut-être une réponse qui arrivera plus lentement, mais ils recevront quand même la réponse. Donc s'ils ont trois résolveurs qui sont correctement configurés et si deux seulement ont la KSK 2010 et un seulement aura la KSK 2017, le service continuera à fonctionner parce que le résolveur pourra utiliser la KSK 2017 et il y aura un résolveur qui fonctionnera.

Donc quel est l'impact sur l'utilisateur final ? Et bien, je veux dire que ce sera plus facile pour les utilisateurs finaux de savoir quel est le résolveur qui fonctionne correctement dans leur cas.

TIJANI BEN JEMAA : Merci beaucoup.

DAVID CONRAD : Une des joies du DNS je dirais, c'est qu'il existe... au niveau du comportement, il dépend de ce que les utilisateurs finaux ont configurés. Donc c'est difficile de savoir ce qui se passe exactement.

Olivier, vous avez la parole.

OLIVIER CRÉPIN-LEBLOND : Merci. Est-ce que vous m'entendez ?

DAVID CONRAD : Oui, on vous entend. Allez-y.

OLIVIER CRÉPIN-LEBLOND : Parfait. J'ai trois petites questions à vous poser. La première est pourquoi est-ce que le roulement de clé a lieu le 11 octobre ?

DAVID CONRAD : Je dirais que quand la communauté a essayé d'identifier la meilleure date en tenant compte des besoins de roulement de clé et de la cérémonie de signature de clé trimestrielle qui doit avoir lieu pour qu'il y ait la zone de signature de clé, nous avons essayé de voir quelles étaient toutes les jours fériés, etc. qui existaient au mois d'octobre 2017. Et la décision a été que le 11 octobre était la meilleure date. Ensuite, nous avons décidé de reporter cela à un an plus tard pour simplifier les choses au niveau de la communauté. Certaines personnes ont proposé de changer les choses, mais bon, on a décidé de garder cette date.

OLIVIER CRÉPIN-LEBLOND : Merci. Bien. Le 11 octobre 2017, ce n'est pas tout à fait pareil que le 11 octobre 2018. Je crois que cela va être un peu plus compliqué. Je voulais savoir s'il y avait des raisons à ce choix.

Ensuite, vous nous avez présenté certaines données, certaines informations dans votre présentation. Il y a un pic dans un graphique que vous nous avez présenté ; il y a un pic le 2 avril ou mois de mars. Est-ce que vous comprenez pourquoi on a ce pic dans ce graphique ?

DAVID CONRAD : Nous avons essayé d'analyser cela. Apparemment, une des raisons qui nous a paru la meilleure était qu'il y avait un logiciel VPN qui faisait un rapport de la KSK originale. Et la raison pour laquelle nous avions ce grand nombre d'adresses IP, la seule source d'adresses IP que l'on voit ici, c'est parce que ce logiciel VPN est une machine qui est connectée sur internet et qui indique qu'ils ont seulement la KSK 2010 configurée. Donc un petit nombre de machines fonctionnaient sur internet et étaient connectées à différents endroits et figurent comme adresses IP uniques. Nous pensons que ce pic se doit donc aux développeurs du logiciel VPN qui nous a envoyé un nouvel ensemble de codes qui a eu un impact sur un plus grand nombre de clients VPN, ce qui les a amené à voir s'il y avait quelque chose qui se passait.

Mais les statistiques qu'ils recevaient à cette époque-là, aux alentours de cette date, elles n'ont pas exactement la direction que l'on souhaiterait. Donc le nombre d'adresses uniques IP qui apparaît était d'environ 20-22 % et on était un petit peu nerveux parce que ce résultat

nous a un peu inquiété et on en a parlé et on a constaté que l'Université de Californie faisait une série de recherches à ce propos et que les choses devraient s'améliorer.

OLIVIER CRÉPIN-LEBLOND : Merci.

Troisième question, je vais être un petit peu provocateur, j'arrive de RIPE. Il y a eu une présentation qui a été faite par une personne. On a parlé du DNSSEC et cette personne disait que si vous le vouliez, vous pourriez faire tout ce que vous voulez au niveau du DNS et vous débarrasser de tout ce qui concerne le DNSSEC. Quelle est votre opinion à ce propos ?

DAVID CONRAD : Il y a eu une suggestion qui a été faite à plusieurs reprises et mon opinion, c'est que le DNSSEC fournit une protection pour les données et pour le transport des données. Et cela protège le transport des données. Alors on a parlé de l'encryptement du DNS qui est spécifié par Dan Bernstein. C'est une technologie qui est très intéressant mais cela protège le transport, pas les données en elles-mêmes.

Mon opinion, c'est qu'il vaut mieux protéger les données. De toute façon, les deux choses devraient être faites. L'avantage aussi de descendre en profondeur les données et le transport des données est important. Cela nous permet de résoudre une série de problèmes. Cela ne résout pas tous les problèmes, cela ne protège pas non plus le cache, c'est la façon dont le DNSSEC le fait. Donc ce n'est pas vraiment une solution si on compare ce système au DNSSEC.

Je vais demander à Russ pour voir s'il a une opinion à ce propos.

RUSS MUNDY : Il y a des analyses qui ont été faites et apparemment, la position des gens qui poursuivent différents types de mécanismes, c'est qu'il y a des recherches qui ont été faites, des tests qui ont été faits, et chacun a sa propre idée de ce qui fonctionne le mieux et en général, ce sont les mécanismes qu'ils connaissent le plus.

Donc en général, on se retrouve face à des faiblesses quelque part, par exemple une alternative de l'approche du système de nom du DNS. Et amener ces gens à vouloir utiliser des technologies, ils avaient besoin de mécanisme de sécurité, genre DNSSEC, donc de toute façon...

ANDREA GLANDON : On vous entend très mal. Est-ce que vous pouvez parler un petit peu plus fort et vous rapprocher de votre micro ?

RUSS MUNDY : Bien, parfait. Oui, je vais essayer. Excusez-moi.

Donc finalement, on doit avoir un mécanisme permettant de faire ce que fait le DNSSEC. Donc il y a, comme David l'a dit, des avantages et des inconvénients pour tous ces systèmes. Et je crois que c'est la meilleure manière de répondre aux questions de gens concernant les différentes technologies. Il faut utiliser plusieurs de ces technologies tout le temps. Merci.

DAVID CONRAD : Je voudrais ajouter aussi qu'une des choses que le DNSSEC fournit et que l'autre système ne peut pas fournir, c'est qu'il s'agit d'un mécanisme qui protège contre des attaques contre le serveur. Le DNSSEC fournit une réponse quand on a une requête pour un nom qui n'existe pas. Cela vous permet de réduire les opportunités pour les attaques malhonnêtes de différents types ou des requêtes qui inondent des serveurs, des requêtes de noms qui n'existent pas. Donc cela permet de fournir une manière d'arrêter des attaques, par exemple l'attaque pour déni de service qui leur permet... Le DNSSEC nous permet de filtrer ce type d'attaques au niveau du résolveur.

Nous avons Hadia qui demande la parole. Hadia, allez-y, vous avez la parole.

HADIA ELMINIAWI : Bonsoir. Nous sommes sur le point de faire ce roulement de KSK 2017. Mais que se passe-t-il si la clé est compromise ? On doit installer cette clé dans la zone racine mais c'est une nécessité. Je voudrais savoir comment est-ce que vous hésitez autant au niveau de la sélection de la KSK 2017 ?

DAVID CONRAD : De mon point de vue, nous hésitons parce que nous jouons un petit peu avec le moteur de l'avion pendant que nous sommes en vol. Donc nous devons faire très attention, quand on a un seul moteur, s'il tombe en panne, l'accident risque d'être grave.

La communauté a proposé un plan très prudent pour faire le roulement de KSK et nous suivons ce plan aussi prudemment que possible. Comme

je l'ai dit pendant ma présentation, il y a des personnes qui suggèrent que l'on fasse le roulement de la KSK plus fréquemment pour pratiquer tout cela et utiliser cette infrastructure.

Personnellement, je propose quelque chose de différent et c'est le rôle des algorithmes, qu'on change les algorithmes. Je pense que l'infrastructure que nous avons construite est solide, mais il y a toujours une possibilité d'avoir une attaque de nouveau type qui va nous obliger à modifier les algorithmes et à trouver des algorithmes qui nous permettraient de lutter contre une attaque particulière. Donc la sécurité est importante ici et je pense qu'il faudra aussi changer les algorithmes installés et mettre en œuvre de nouveaux algorithmes. Merci.

Alan ?

ALAN GREENBERG : Merci. Un des commentaires qui a été fait par ALAC était de demander à ICANN de fournir une URL qui permettrait à quelqu'un de faire ce type de requête dont vous parlez et de vérifier si le résolveur qui est utilisé était activé pour le DNSSEC.

La communauté n'a probablement pas activé ce système. Et si vous savez que votre résolveur n'est pas activé pour le DNSSEC, cela augmente la pression dans une région donnée.

Maintenant, on peut se demander que faire si on n'a pas le DNSSEC activé. Qu'est-ce qu'il faut faire ? Ce que l'on essaie de faire ici, c'est qu'ICANN fournisse quelque chose qui ne demande rien de très technique et qui permettra à n'importe qui de comprendre la réponse qui sera fournie et de donner des explications, une aide pour qu'un

utilisateur qui appelle son fournisseur d'internet et lui demande à propos de la KSK, cette personne qui va lui répondre doit être au courant aussi. Donc on a besoin de quelque chose qui permette aux gens de savoir ce qu'ils doivent demander, ce qu'ils doivent répondre. Il y a une série d'utilisateurs dans le monde entier, qui appartiennent à At-Large ou pas, qui pourraient faire ce type de tests et alerter leur fournisseur s'ils détectent le problème de DNSSEC non-activé.

Donc il nous faut avoir une URL qui nous permettrait d'envoyer un message technique et de savoir que faire et qu'est-ce qu'il faut faire en cas de problème. Je voudrais qu'ICANN propose quelque chose pour soulager un petit peu la pression et pour fournir une aide, un guide aux personnes qui n'ont pas ce système de DNSSEC activé sur leur propre système.

DAVID CONRAD : Merci Alan. Cette question concernant quoi faire pour les utilisateurs finaux a été prise en compte par l'organisation, par la communauté technologique et technique que nous avons consultée.

Et une partie des défis qui avaient [inintelligible] ici, c'était qu'à l'origine, au sein de l'organisation, nous avions proposé de dire aux utilisateurs finaux de joindre leur fournisseur d'internet et de leur demander. Mais beaucoup de gens ont pensé que c'était une très mauvaise idée parce qu'à ce moment-là, les fournisseurs d'internet allaient être inondés de question. Et la personne qui posait la question [n'avait pas intérêt] à comprendre ce qu'elle devait poser comme question ou comprendre la réponse. Et si elle comprenait la réponse,

une question allait être suffisante. On n'avait pas besoin d'avoir une ligne de soutien pour ce type de questions.

Donc présenter un outil, c'est quelque chose dont nous avons parlé au niveau interne. Et les défis qui existaient à l'époque existent toujours. On peut dire à distance si les validateurs de DNSSEC sont activés dans un système. On peut donner des systèmes pour savoir si le DNSSEC est activé.

Mais comme vous l'avez dit, nous devons réduire le type de problèmes sur lesquels le public va devoir se renseigner et les fournisseurs d'internet devraient pouvoir, à travers une adresse sur Google, savoir où est-ce qu'il en est, savoir si le DNSSEC est activé sur son système. L'utilisateur final sera dans une position où il ne sera pas obligé d'envoyer toutes ses questions à son fournisseur. Les fournisseurs peuvent se fatiguer rapidement de recevoir ce type de questions.

Donc nous luttons encore pour savoir que faire si l'on découvre que le fournisseur d'internet fait les bonnes choses au niveau de la validation mais vous ne le savez pas. C'est quelque chose dont nous sommes en train d'essayer de voir.

ALAN GREENBERG : Nous aurons une session à Panama et nous pourrons en parler.

DAVID CONRAD : Andrei ?

ANDREI KOLESNIKOV : Merci. J'ai une question à laquelle peut-être vous, Russ, pourrez répondre si pas vous. Je pense qu'il y a ici une question qui comporte deux aspects. Est-ce que les difficultés sont posées au niveau des résolveurs ou alors est-ce vos algorithmes cryptographiques pourraient être problématiques ? Donc quelle serait la portée ?

DAVID CONRAD : En fait, que je sache, c'est au niveau de l'algorithme qui est utilisé que l'on a ce problème. Donc utilisant cet algorithme, il est fort improbable qu'il puisse être attaqué [sans] technologie. Autrement, le RSA est vulnérable à la cryptographie quantique. Donc il y a des personnes qui considèrent cela un risque.

Donc l'un des défis de l'algorithme existant est que les signatures sont très longues et qu'il est de plus en plus difficile... On finit par avoir des plus grands paquets qui provoquent des problèmes, en particulier avec l'IPv6. On souhaite donc passer à un algorithme tout neuf qui ait de meilleures caractéristiques pour ce qui est de la résistance aux attaques cryptographiques mais qui a également des signatures bien plus courtes, la moitié de la taille. Donc cela simplifierait bien les choses du point de vue opérationnel.

TIJANI BEN JEMAA : Merci David.

DAVID CONRAD : Il me semblait qu'il y avait d'autres questions.

TIJANI BEN JEMAA : Non, je ne vois plus d'autres mains levées. S'il n'y a plus d'autres questions, je vais demander à Andrea de passer l'interrogation.

ANDREA GLANDON : Merci. Alors l'interrogation.

Première question. Comme vous voyez à la droite de l'écran en vas. Pourquoi est-il important de changer la clé, la rouler ? Vous pouvez saisir la réponse et puis l'envoyer avec le bouton que vous avez juste à côté de la case blanche.

On a les résultats. David, vous pouvez les consulter. Est-ce que vous voyez les réponses, David ?

DAVID CONRAD : Oui. On continue de recevoir des réponses. Donc les réponses envoyées comprennent la sécurité du DNS [inintelligible] bon pour la sécurité ; des questions de sécurité ; motivation pour se conformer à la directive communautaire de changer tous les cinq ans ; et puis pour éviter [inintelligible] ; et puis pour renforcer l'infrastructure au cas où on aurait besoin de changer la clé. Si [inintelligible] fonctionne correctement, c'est comme si on changeait un mot de passe fréquemment. Des fois, cela est considéré une bonne pratique cryptographique.

ANDREA GLANDON : Très bien. On passe à la question suivante. Qu'est-ce que le DNSSEC empêche-t-il ?

Saisissez la réponse dans la case blanche avant de l'envoyer. Je vais montrer les résultats, David, pour que vous puissiez les voir à mesure qu'ils arrivent, à mesure qu'on reçoit les réponses. On a trois réponses jusqu'à présent. David, est-ce que vous pouvez les voir ?

DAVID CONRAD : Oui, je les vois, effectivement. On vient d'en recevoir une quatrième, d'ailleurs.

ANDREA GLANDON : Très bien. Allez-y, vous pouvez voir les réponses.

DAVID CONRAD : Donc réponses : empoisonnement de cache, c'est un risque ; quelque chose en Français j'assume ; le DNSSEC protège les données en elles-mêmes, donc cela empêche la modification des données.

Je serais probablement d'accord avec cette dernière partie. Cela protège les données en elles-mêmes, donc cela empêche la modification des données. C'est comme cela qu'on empêche l'empoisonnement de cache. Voilà une bonne réponse. Et bien sûr, des mauvaises actions [inintelligible], c'est toujours une bonne réponse aussi.

ANDREA GLANDON : D'accord. On va passer à la question suivante.

Tijani, est-ce que vous voulez conclure l'appel ? C'était la dernière question.

TIJANI BEN JEMAA : Oui. Merci Andrea.

Est-ce qu'on peut voir les questions qui nous reste, les questions d'évaluation ?

ANDREA GLANDON : Bien sûr.

Que pensez-vous par rapport à l'heure à laquelle ce séminaire web a été prévu ? Est-ce a) trop tôt ; b) correct ; c) trop tard ?

On passe à la deuxième question dans un instant. Que pensez-vous par rapport à la technologie utilisée pour le séminaire web ? Est-elle a) très bonne ; b) bonne ; c) suffisante ; d) mauvais ; ou e) très mauvaise ?

Question numéro 3. Les présentateurs maîtrisaient-ils le sujet ? Leurs connaissances étaient a) extrêmement fortes ; b) fortes ; c) suffisantes ; d) faibles ; ou e) extrêmement faibles ?

Question suivante. Êtes-vous satisfait de ce séminaire web ? a) extrêmement satisfait ; b) satisfait ; c) modérément satisfait ; d) légèrement satisfait ; ou e) complètement insatisfait ?

Question suivante. Dans quelle région habitez-vous en ce moment ? a) Afrique ; b) Asie, Australie et les îles du Pacifique ; c) Europe ; d) Amérique latine et les Caraïbes ; ou e) Amérique du Nord ?

Finalement, combien d'années d'expérience avez-vous au sein de la communauté de l'ICANN ? a) moins d'un an ; b) deux ou trois années ; c) de trois à cinq ; d) de cinq à dix ; ou e) plus de dix ans ?

Et dernière question. Quels seraient les sujets que vous aimeriez que nous abordions dans les séminaires à venir ?

Merci Tijani, voilà toutes les questions d'évaluation.

TIJANI BEN JEMAA : Merci bien, Andrea. Cette question est importante ; il est important que vous y répondiez. Si vous n'y répondez pas maintenant tout de suite dans le séminaire web, envoyez-nous un mail pour nous faire savoir quels sont les sujets qui vous intéressent pour les séminaires web à venir, de manière à ce que l'on puisse mieux planifier notre programme pour l'année prochaine.

Merci à tous. Je commencerai par remercier David de sa présentation qui est formidable et de toutes ses réponses à nos questions. Je remercie notre personnel, nos interprètes et vous tous qui avez assisté à ce séminaire web.

Merci à tous. Ce séminaire web est maintenant conclu.

DAVID CONRAD : Merci à tous. Au revoir.

ANDREA GLANDON : Merci. Nous voilà à la fin de l'appel. Rappelez-vous de déconnecter toutes les lignes et bonne fin de journée. Au revoir

[FIN DE LA TRANSCRIPTION]