SAN JUAN – Mise à jour sur le roulement de la KSK
Mercredi 14 mars 2018 – 16h15 à 16h45 AST
ICANN61 | San Juan, Porto Rico

NON IDENTIFIE: Nous allons passer à la présentation sur le roulement de la KSK très bientôt. Si on pouvait mettre la présentation à l'écran, merci. Nous allons commencer dans 30 secondes.

HOWARD BENN: Bonjour à tous, bienvenus à la séance sur la mise à jour du roulement KSK. J'espère qu'il y a quelqu'un dans la sale qui ne m'a pas entendu faire cette présentation lors de cette réunion ICANN. Je vais quand même commencer par faire un récapitulatif de la situation courante

Si vous avez un intérêt sur ce sujet et que vous êtes dans cette salle, le roulement devait être fait mais a été retardé parce que VeriSigne a analysé le RFC8445 et a trouvé qu'il y avait à peu près 7 à 8 % des résolveurs qui avaient seulement le KSK 2010, et qui n'avaient pas donc la nouvelle version. Donc quelque chose ne fonctionnait pas bien avec ces 7 à 8 % des résolveurs.

Donc le bureau du CTO a répété cette analyse en étudiant les trafics entre différents serveurs, et nous avons trouvé les mêmes

résultats. Le pourcentage était à peu près le même. C'était tout de même un pourcentage assez important et nous n'en comprenions pas non plus la raison pour laquelle ces résolveurs ne fonctionnaient pas.

Donc nous avons décidé de faire une pause et de reporter ce roulement, ainsi d'avoir le temps de déterminer la raison pour laquelle il y avait un problème.

Nous avons donc fait une étude au mois de septembre. Nous avons essayé de faire un suivi pour savoir exactement ce qui se passait. Et nous savions déjà qu'il y avait un problème. Nous avons pu contacter seulement à peu près 20 %, cela fait à peu près 100 adresses. La majorité était des adresses qui étaient connues par des machines éphémères. Il y avait aussi le fait que le signal était envoyé comme une requête DNS.

Nous savons que le transfert était effectué, mais nous nous sommes rendu compte que ces résolveurs avaient le KSK 2010, donc il n'y avait pas de… Nous pouvions donc ainsi parler avec les vendeurs des résolveurs, mais ce n'était pas facile.

Donc sans parcours à suivre pour l'avenir, l'organisation et de recherches que nous pouvions conclure, l'ICANN nous a demandé de reporter. Nous allons continuer à recevoir des contributions et à faire des recherches.

Il y a donc un groupe qui s'est dédié à faire ces recherches. Je suppose que si vous n'êtes pas sur cette liste de distribution, faites-le, puisque vous pourrez ainsi obtenir des informations.

Il y avait un accord, il y a un accord entre nous, il n'y avait pas de bonne manière de mesurer les choses. L'équipe de conception que ICANN a réunie il y a deux ans, a déjà fait un rapport sur des recommandations du roulement de KSK. Ils ont dit qu'une bonne mesure serait de voir combien d'utilisateurs ont été affectés pour pouvoir savoir s'il y avait des problèmes significatifs.

Donc il est très difficile de mesurer de la sorte. Nous espérions qu'il y aurait des mesures plus plausibles pour l'avenir, et ils s'attendaient à un système que l'on aurait appelé Sentinel, qui vient de Google. Et il y a des personnes qui travaillent là-dessus en utilisant donc des mesures basées sur les utilisateurs.

Le consensus de ce groupe était que l'ICANN devrait faire le roulement de la clef dans les délais et c'est ainsi que nous avons fait. Nous avons essayé de continuer de faire de la sensibilisation sur le sujet.

Nous avons publié un plan, c'est une version préliminaire pour le roulement KSK. Tout d'abord, nous avons dit que nous allons le retarder d'un an, nous allons le faire le 11 octobre 2018. Nous espérions pouvoir étudier les nouveaux critères pour mesurer. Si

quelqu'un a des suggestions sur des critères spécifiques, nous voulons continuer à communiquer sur ce sujet.

Nous allons publier des observations supplémentaires, surtout par rapport au RFC8145. Je ne pense pas que nous avons assez de preuves pour pouvoir expliquer ce qui s'est passé. Les documentations que nous avons ne sont pas forcement pertinentes au projet.

Nous avons une période de commentaires qui est ouverte puisque pour l'instant nous en sommes à une version préliminaire du plan. Nous voulons vraiment avoir des contributions de la communauté sur cette proposition.

Cette période de commentaires va être fermée le 2 avril et voilà sur l'écran le lien, l'URL pour la page concernée.

Si nous continuons avec ce plan, et avec les délais de ce plan, cela ressemblera à ce que vous voyez à l'écran. Le 2 avril vous aurez donc la fin de la période de commentaires, à la mi-avril le rapport du personnel sera publié. Nous aurons aussi une révision du plan si c'est nécessaire, et nous publierons ces résultats.

Si vous n'êtes pas familier avec la cadence des réunions de l'ICANN, nous nous réunissons trois fois par an et entre ces

réunions, il y a des groupes de travail, des ateliers de travail du conseil.

Donc durant la prochaine réunion de l'atelier de réunion du bureau de l'ICANN sera au mois de mai et nous allons demander à ce qu'il y ait une résolution soit faite et qu'une communication soit faite à RSSAC et SAC et que ces deux groupes puissent faire des commentaires.

Donc d'ici le premier octobre nous aurons donc une discussion à Panama et nous parlerons encore une fois du roulement de la KSK, de la KSK de la racine. Ainsi nous pourrons faire des révisions du plan.

Si les révisions ne demandent pas à ce qu'il y ait un changement de date, donc quand nous parlons du 11 octobre 2018, nous continuerons sur ces délais. Et ensuite nous demanderons à l'ICANN de faire le roulement de la clef le 11 octobre 2018.

Voilà où nous en sommes et voilà où nous allons. Nous avons vraiment besoin des contributions de la communauté. Nous voudrions que les gens fassent part de leurs informations sur le commentaire public.

Je vais parler maintenant des signaux que nous recevons à travers le RFC 8145. Pour l'instant, le bureau du CTO a l'accès

donc à ce RFC 8145. Vous voyez sur l'écran les 12 serveurs racine. Nous avons ajouté H à la liste des serveurs.

L'analyse initiale qui a été faite à la fin 2017 a utilisé des données [pecap] de B, D et F. Depuis, nous avons utilisé la méthode de [Dowain Vassaux] sur le DNX cap. Et cela analyse le trafic en temps réel. Toutes les 60 secondes il y a un rapport qui est fait sur chaque batche. Et comme vous le voyez sur l'écran les statistiques sont énoncées. Il y a donc des requêtes DNS vers une zone, une zone opérée par l'ICANN, le bureau du CTO de l'ICANN, comme vous le voyez à l'écran.

Nous avons des encres de confiance qui sont notées en 4 chiffres, vous avez différents codes comme le 4F66, vous avez l'identification de la zone racine. Et quand on se base là-dessus, on peut donc établir le diagramme que vous avez sur l'écran, ou le graphique. Comme vous voyez, nous avons de plus en plus de rapports de la part des serveurs.

Je vais expliquer ce graphique. Les trois lignes que vous voyez correspondent à trois choses différentes. Les lignes rouge et verte reportent le nombre des IP. Et vous le voyez sur l'écran, vous voyez que la ligne verte correspond au nombre total des sources. Ce sont des sources uniques par jour. Comme vous le voyez maintenant, nous sommes à 55 000 adresses uniques qui font des rapports tous les jours.

La ligne rouge correspond aux numéros, aux chiffres, aux numéros qui n'ont que les vieilles clefs. Donc si vous divisez la rouge par la verte, vous avez un pourcentage qui est représenté par la ligne noire et qui correspond au pourcentage des sources qui font leur rapport seulement à la KSK 2010.

Il faut voir qu'il y a donc une grosse hausse en janvier, parce qu'il y a eu pus de rapports de faits. Donc le pourcentage a augmenté. Nous sommes presque sûrs que c'est le résultat de la mise à jour des Unbound. Le unbound 168 a été émis en janvier. Et ceci a été fait pour faire face à sécurité, c'était un patch sécurité, et tout le monde était motivé pour faire cette mise à jour.

Il n'y a pas de baisse de KSK 2010 après 30 jours. Si quelqu'un n'utilise pas l'outil d'encrage Unbound… attendez je vais le dire différemment : si quelqu'un fait une mise à jour du Unbound et n'utilise pas l'outil Unbound, ils vont tout de suite mettre à jour leur encrage avec les bonnes données.

Il est commun de faire la mise à jour sans utiliser l'encre unbound, et que la configuration soit faite avec la vieille clef. Mais après 10 jours, le processus devrait être utilisé.

Pourquoi y a-t-il un problème ? Une des hypothèses est celle-ci : si ce sont des machines virtuelles et qu'il y a une vieille clef, le rapport donc - enfin quand je parle de vieille clef, je devrais

parler de la KSK 2010 – donc dans ce cas, si cela fonctionne pendant quelques jours, et qu'elle s'arrête, elle n'a pas le temps de faire le travail. Donc quand cela se reproduit plusieurs jours après, cela revient en arrière et réutilise la KSK 2010.

Et nous n'avons pas fini les diapositives parce que nous avons dû venir à Puerto Rico, nous n'avons pas eu le temps de finir la présentation.

Donc maintenant nous avons sur l'écran le rapport. Nous devons faire des rapports sur les cadences régulières. Il y a des IP qui ne fonctionnent pas dans ce sens. On assume qu'il y a des problèmes. Et c'est pour cela que nous faisons de plus amples recherches pour essayer de comprendre le problème.

Voilà notre graphique pour les serveurs racine individuels. Ces graphiques correspondent aux 11 serveurs dont nous avons des données. Vous voyez qu'il y a des serveurs où nous avons des données à des périodes de temps différentes.

Si vous voyez ces graphiques, ils sont assez similaires, excepté pour la racine J. La racine J fonctionne à peu près mieux que les autres, du moins c'est ce qu'on voit à travers les pourcentages.

Il n'y a pas tellement de différences de données entre les différents serveurs de racine. Ce qui est important c'est de voir le changement de comportement qui a lieu en mi-janvier, quand il

y a eu cette hausse. Comme vous voyez sur ces graphiques, vous voyez que les adresses IP uniques sont ajoutées tous les jours. Combien de sources font des rapports de données par rapport aux rapports que nous avions auparavant ? Vous voyez que nous avons des centaines de nouvelles IP tous les jours. Il y a eu des mises à jour qui ont été faites en janvier, donc vous voyez beaucoup plus de sources uniques qui font des rapports tous les jours.

Si vous deviez mettre en place un graphique sur les cumuls de ce que nous voyons tous les jours, ce serait ce graphique-là. Comme vous le voyez sur l'écran. Vous voyez combien d'IP uniques cumulatives tous les jours.

Nous voyons de plus en plus d'adresses uniques. Maintenant nous en sommes à 700 000 et plus d'adresses uniques. C'était donc la conversation que nous avons eue avec les adresses qui ont fait leur rapport. Beaucoup d'entre eux nous ont dit qu'ils n'avaient que le KSK 2010. Il s'agit de 35 % des adresses au total, des rapports des adresses totales par rapport au KSK 2010.

J'ai décidé d'observer les 24 S uniques. Vous voyez qu'il y a une augmentation en janvier. Après ça a stagné un peu, mais malgré tout, nous avons encore beaucoup de hausses. Nous en sommes à 350 000, et ça c'est une moyenne. C'est une moyenne de 2 IP par slash24. Ça indique qu'il y aurait des blocs avec beaucoup

d'adresses et nous pouvons donc faire des recherches sur cela. Cela correspondrait peut-être à des dynamiques de machines.

Voilà, cela correspond à beaucoup d'adresses. Le nombre total des adresses qui font leur rapport soit KSK 2010 ou KSK 2010 et 2017, nous savons que ce chiffre est plus important que les IP uniques. Ils ont fait le rapport sur le KSK 2010, et ensuite ils ont fait le rapport en disant : j'ai le KSK 2017, pas forcement dans cet ordre, mais ils ont fait le rapport.

Une des raisons pour laquelle ça fonctionne ainsi, donc ce rapport 2010 et ensuite ce rapport 2017, c'est que cette machine a fait sa mise à jour, et maintenant elle a cette nouvelle KSK.

Donc sur ces trois quarts de million d'IP, seulement un certain nombre font ce rapport. Et un des problèmes ici c'est qu'il y a un problème avec le signal. Parce que vous voyez un rapport de l'IP de source, vous n'avez pas de garantie de la configuration de cet IP. Cela pourrait être quelqu'un qui fait le transfert vers cet IP et qui ensuite transfère vers un serveur racine. C'est là que nous voyons l'information. C'est pour ça que nous voyons seulement une source unique qui fait le rapport de 2010 et pas de 2017. Nous savons aussi qu'il y a des mises en œuvre qui ont été faites, et nous avons des données qui n'ont pas forcement validé s'ils avaient KSK 2010, ça n'aurait aucune importance. Donc la configuration a été faite, mais ça n'avait aucune importance.

Donc si vous voulez regarder ces graphiques pour vous-même, sachez qu'il y a une mise à jour régulière, vous pouvez y avoir accès sur ICANN.ORG, l'adresse figure ici à l'écran.

Je viens de commencer à présenter les données de cette manière, ça c'est basé, ce tableau en particulier est basé sur les IP qui ont fait un rapport sur le KSK 2010, mais sur un nombre plus limité, je ne me souviens plus du nombre exact, mais ici vous voyez le nombre de systèmes autonomes, de sorte que les ASN, numéros de systèmes autonomes… excusez-moi il ne s'agit pas simplement du KSK 2010, mais de tous les ASN qui font un rapport. Donc ce serait un tableau différent si vous vouliez obtenir simplement le KSK 2010.

Le fait est que.. Bon il faut que je revois ce tableau pour reprendre uniquement les chiffres du KSK 2010, pour voir ce qu'il se passe avec les ASN qui ont des résolveurs qui font rapport uniquement sur le KSK 2010.

Nous avons distribué une liste d'adresses IP qui font rapport uniquement sur le KSK 2010 à l'ISPCP et aux RIR, et l'idée ici c'est d'améliorer ces deux systèmes, mais ce qui nous intéresse beaucoup, c'est de savoir ce qu'il se passe et pourquoi il n'y a pas une mise à jour de ce système. Par exemple l'un des meilleurs résultats ce serait de s'apercevoir qu'il y a effectivement un espace d'adresses, où l'ancienne configuration

avec l'ancienne clef pourrait fonctionner. Ca, ce serait une bonne découverte.

Cette diapo est maintenant obsolète. Je suis maintenant autorisé à l'ICANN pour actualiser une page qui va ressembler à celle-ci avec les ASN actualisés avec toutes les adresses faisant rapport sur le KSK 2010. Donc ce sera beaucoup plus simple qu'un opérateur donné puisse s'y retrouver. Et bien entendu nous allons contacter les opérateurs, à commencer par ceux qui font rapport sur le KSK 2010 pour voir ce qu'il se produit.

Quelles sont les prochaines étapes ? Continuer à voir ce qu'il se passe par rapport au RFC 8145 et les données y afférentes. Mais même si ces données ne me satisfont pas, ce sont les seules dont nous disposons pour l'instant, ce sont celles qui vont nous permettre de voir ce qu'il se passe, et ça, en soi, c'est une bonne découverte.

Donc on va essayer de prendre contact avec les réseaux qui ont fait rapport d'un grand nombre de résolveurs du KSK 2010. On va enquêter et on va continuer à parler de cela. Donc vous allez continuer à me voir, moi-même et mes collègues, et on va continuer à informer la communauté, parce que comme je l'ai dit, on a besoin de votre aide.

Donc n'hésitez pas à faire des commentaires sur le projet de plan, vous voyez ici le lien à l'écran, et vous pouvez également souscrire à la liste de diffusion qui figure ici à l'écran.

Et avant de nous quitter, j'ai encore deux petites minutes, trois petites minutes, s'il y a des questions dans la salle.

HOWARD BENN: Bonjour Howard Benn, de Samsung Electronic au mmicro. Alors par rapport à la diapo que vous avez montrée avec tous les opérateurs… Oui, celle-ci. J'ai le sentiment que le réseau, qui doit être le réseau LTE, est opéré exclusivement sur des machines, et donc vous n'allez jamais parvenir à la limite des 30 jours.

Donc il serait très intéressant de voir si les opérateurs de téléphonie mobile sont confrontés aux mêmes problèmes ou pas.

Mais là encore, je peux vous donner des informations de contact, parce qu'on utilise précisément ces équipements.

NON IDENTIFIE: Bien, merci.

MARK: Bonjour, je représente les FSI, mais je parle en mon nom propre.

Est-ce qu'on peut revenir à la diapo numéro 4 ? Oui, celle-ci.

Alors, moi ce qui m'intéresse c'est la fin de cette diapo, résultat de la discussion, premier et troisième point. Peut-être que je me trompe, mais le premier point dit : on ne connait pas les effets que cela va avoir sur l'internet. Et le troisième point dit qu'il faut le faire de toute façon. Est-ce que j'ai bien compris ?

NON IDENTIFIE: Alors ça se serait l'interprétation un peu pessimiste.

NON IDENTIFIE: Non, je pensé que le reste de la présentation ce serait une interprétation plus optimiste.

Alors plus sérieusement, il s'agit d'un problème complexe, on ne sait pas comment le prendre. Et, à l'automne dernier nous avons décidé qu'il fallait impliquer la communauté. Et que la communauté participe. Et le résumé que vous venez de faire c'est ce que nous a dit la communauté.

Mais les gens qui participent au roulement KSK sont des conseillers au DNSSEC et tous ceux qui participent au DNSSEC, donc qui souhaitent qu'il y ait un roulement KSK, donc voilà le sentiment qu'on avait. Mais c'est pourquoi les contributions et les commentaires publics sont si importants.

MARK: Merci, et merci de cette explication. Mais je continue à avoir un point de vue pessimiste ici. Et je sens que là je suis en train de plaider en faveur du DNSSEC, mais je n'arrive pas à dépasser les points 1 et 3. Comment est-ce qu'on peut proposer d'introduire un changement dans la zone alors que vous ne savez pas quels vont en être les effets ?

Je suis d'accord avec vous, et je fais tout à fait confiance à votre analyse par rapport à la mauvaise qualité du signal que vous recevez. Et, avec le temps qui passe, le signal que vous recevez, qui est la seule information en terme de diagnostic que vous obtenez, ce signal empire.

Et là encore, je caricature un petit peu la situation.

Toutes les diapos suivantes sont frappantes, mais cette diapo en particulier, sous l'intitulé résultat de discussions point 1 et trois, je n'arrive pas à les saisir. Pourquoi, alors qu'on n'en connait pas les effets, quelqu'un dans la communauté dirait : oui, oui, allez y continuez, allez de l'avant ,alors qu'on ne connait pas les effets.

Mais en tout cas merci de vos explications.

NON IDENTIFIE: Alors, permettez-moi de vous faire part d'une autre interprétation, ce n'est pas la mienne d'ailleurs, mais je vous en fais part quand même. Parce qu'il y aurait un inconvénient à ne pas déployer ou rouler la clef.

Parce qu'il y a des menaces actuellement vis-à-vis de la cryptographie ou aux opérations physiques de la sécurité. Et le fait de ne pas rouler la clef, ça pourrait entrainer des menaces vis-à-vis de la clef.

Donc si on n'arrive pas à régler toutes ces menaces rapidement, il pourrait y avoir des coupures, et donc il faut rouler la clef.

MARK: Je comprends bien votre argument. Vous dites oui, ce qu'on veut faire c'est rouler la clef parce qu'on veut que les gens aient confiance dans le DNSSEC. Je comprends bien la logique de cela.

Mais d'un autre côté, si on se trompe, et je suis frappé ici qu'on soit en train d'être approximatifs et on ne travaille pas avec des certitudes, c'est que jusqu'à présent on ne l'a pas fait dans la vie réelle, mais on a un problème de réputation ici dans les deux cas.

Et ça place l'ICANN dans une situation délicate. Pour ma part, je ne suis pas convaincu du fait que le problème du déséquilibre de

la réputation du DNSSEC c'est la même chose qu'avancer à l'aveuglette sur quelque chose qu'on ne connait pas.

NON IDENTIFIE: Y a-t-il d'autres commentaires ? Est-ce qu'on a quelque chose sur le chat ? Non ? Dans la salle.

NON IDENTIFIE: Merci. Ma question est la suivante. On a découvert au Nigéria, parce qu'on a 4 entreprises opérateurs de téléphonie mobile et de grands FSI, et seul un fournisseur de téléphonie mobile utilise le DNSSEC sur ces 4. Les trois autres opérateurs de téléphonie mobile ont d'autres systèmes de validation autres que DNSSEC.

Donc ma question est la suivante : quels sont les avantages du DNSSEC par rapport à d'autres systèmes de validation de sécurité ? Et est-ce qu'il faut réellement que les trois autres opérateurs de téléphonie mobile passent au DNSSEC ensuite ?

Que se passe-t-il pour les autres opérateurs de téléphonie mobile qui n'utilisent pas le DNSSEC pour passer au roulement de la clef.

NON IDENTIFIE: Est-ce que vous pouvez répéter votre dernière question s'il vous plait ?

NON IDENTIFIE: Oui, ce que je dis, c'est que les trois autres opérateurs de téléphonie mobile n'utilisent pas le système de validation DNSSEC.

Donc qu'est-ce qu'il en est du roulement de la clef ?

INTERPRETE : L'intervenant répète, mais l'opérateur ne comprend pas le mot en anglais.

NON IDENTIFIE: Donc quelle serait l'incidence en terme de roulement de clef ?

NON IDENTIFIE: Alors il n'y a pas d'impact du tout. C'est le sentiment et l'opinion de l'ICANN que le DNSSEC est un bon système de validation, donc on encourage les gens à avoir recours à ce système de validation.

D'ailleurs, monsieur excusez-moi, mais je ne me souviens pas de la première partie de la question.

NON IDENTIFIE: Est-ce qu'il y a des avantages pour ceux qui n'utilisent pas le DNSSEC à commencer à utiliser le DNSSEC ?

NON IDENTIFIE: Oui, la position de l'ICANN c'est qu'il faut, on devrait faire un système de validation DNSSEC, parce qu'avec le DNSSEC on est sûr que la réponse que vous recevez répond réellement à la question que vous avez posée et que cette réponse provient bien de qui vous pensez qu'elle provient. Donc vous avez cette assurance du fait que la réponse que vous obtenez provient bien de l'endroit où vous l'avez demandée.

Donc ça vous garantit que cette réponse provient bien de là et qu'elle n'a pas été modifiée. Donc ça vous offre un niveau de garantie et d'assurance plus élevé le DNSSEC.

Sans le DNSSEC, vous êtes plus vulnérable à l'hameçonnage ou à l'usurpation d'identité. Plutôt usurpation d'identité.

NON IDENTIFIE: Y a-t-il d'autres questions dans la salle ? Bien, merci d'être venu.

[FIN DE LA TRANSCRIPTION]