ABOU DABI – Réunion conjointe du Conseil d'administration de l'ICANN et du Groupe d'experts techniques (TEG)
Mercredi 1 novembre 2017 – 17h00 à 18h30 GST
ICANN60 | Abou Dabi, Émirats arabes unis

DAVID CONRAD: Puis-je demander aux autres membres du conseil de venir nous rejoindre ici, s'il y a encore quelques places.

Merci Markus et Becky.

Ok. Bien, je pense qu'on va commencer, soyez les bienvenus à cette réunion du comité technique expert. Donc des experts techniques qui se réunissent avec le conseil d'administration de l'ICANN.

Et cette année en particulier, nous avons une nouveauté, à savoir la création du comité technique du conseil d'administration ;

Ce conseil technique du conseil d'administration, je crois que c'était une réunion obligatoire pour ce BTC, comité technique du conseil d'administration.

Donc, dans un intérêt de temps, j'aimerais vous dire que la raison pour laquelle je porte une cravate aujourd'hui, ça n'est pas parce que j'ai des interviews, mais plutôt parce que lors de

la dernière réunion Steve, pour le TEG, donc j'aimerais dire personnellement Steve, que j'ai énormément apprécié de travailler avec vous, d'avoir créé ce groupe, et de l'avoir conduit jusqu'à ce que le CTO soit créé.

Mais je vous remercie, Steve, des efforts que vous avez fait pour améliorer l'aspect technique de l'organisation et pour m'avoir aidé et avoir aidé le CTO à améliorer l'aspect technologique et bien d'autres aspects de l'organisation.

Su r ce, à moins que vous souhaitiez répondre…

STEVE CROCKER: Oui, merci de vos paroles bien aimables.

Effectivement, la bonne nouvelle c'est que ça fait longtemps que vous êtes avec nous et que vous êtes encore avec nous.

Ce groupe, groupe technique d'experts, a été créé de manière un peu surprenante, mais est devenu une source supplémentaire d'expertises et de créativité aussi. Et a permit d'organiser des discussions qui, dans un autre espace, n'auraient pas pu avoir lieu.

Donc je suis heureux que ce groupe ait été créé, et je suis sûr que nous partageons cela avec les autres.

Donc voilà ce que l'on peut retenir. Et David, je dois le dire, a très bien assumé les aspects administratifs, et les aspects de fonds en réunissant autour de lui les bonnes personnes. Donc ça a été vraiment très agréable de travailler avec vous.

DAVID CONRAD: Sur ce, je pense que l'on peut commencer. Première présentation par Fernando Lopez sur les identifiants du DNS, ce sera une démonstration.

Il s'agit d'un prototype qui utilise les identifiants persistants similaires à ce qu'on appelle le DOA ou l'architecture des objets numériques.

Je crois que cette présentation va être faite en espagnol, donc les interprètes, si vous ne comprenez pas l'espagnol, vous aideront avec l'interprétation.

Et Alain veut intervenir ?

ALAIN DURAND: Merci David. Je vais présenter les premières diapos qui vont présenter la démonstration.

Donc je vais parler en anglais. Je pourrais parler en français, mais je ne suis pas sûr de bien me faire comprendre.

Alors, est-ce que les diapos sont à l'écran ?

Oui, je vais vous demander de bien vouloir afficher la présentation à l'écran s'il vous plait.

Bien je vais commencer par quelques clauses de non-responsabilités. C'est un travail que le CTO a commencé il y a un certain temps maintenant et l'objectif est de démontrer si les identifiants persistants tels que DOA peuvent être atteints uniquement avec le DNS.

Donc, dans cette présentation, je vais vous montrer le type de prototype qu'on a élaboré en collaboration avec l'université de La Plata. Fernando va en parler un peu plus en détail.

Il ne s'agit pas de l'approbation du DOA, de la technologie DOA de la part de l'organisation ICNAN, ça c'est important à souligner.

Donc le contexte de persistance est le suivant. Il était dit qu'il y a des changements organisationnels, des fusions/acquisitions et après 15, 18 mois, 24 mois, un certain nombre d'URL ne fonctionnent plus.

Donc, il y a un certain nombre de solutions qui ont été trouvées, comme les « redirects » URL et autres.

On a étudié les identifiants persistants par le système Handle. Donc si on n'utilise pas des noms, on n'utilise pas quelque chose qui est attaché d'un point de vue sémantique à cela. Donc l'idée c'est que si l'organisation change, le nom peut être le même. Le nom peut rester intact.

Si c'est un numéro, ça n'est pas aussi important.

Par rapport à l'aspect suffixe, plutôt que d'avoir une structure en profondeur d'une entreprise, on recommande d'utiliser un espace plat, a flat space, et pas hiérarchique.

Donc on utilise des protocoles spécifiques qui ne sont pas normalisés tels que l'IETF. Et on ne regarde pas simplement les protocoles et les identifiants persistants.

Et les identifiants persistants ce sont le résultat d'une convention de nommage.

Donc, est-ce qu'on peut faire avec le DNS ? Notre réponse la plus courte, c'est oui. On a besoin de trois choses.

Un endroit dans le DNS pour ancrer, donc c'est ce qu'on appelle l'ancrage de persistance.

On a besoin d'une convention de nommage qui est semblable à celle que j'ai décrite plus haut. Donc dans les étiquettes de DNS, n'utilisez pas un nom ou quelque chose qui a à voir avec la

sémantique. Vous pouvez utiliser un numéro ou un symbole, mais pas un nom. Et dans structure de l'organisation, utiliser autant que possible des espaces plats.

Nous avons introduit un nouveau type d'enregistrement pour les données, appelé DTA. Et ça n'a pas besoin d'être une cartographie d'un nom vers une adresse IP, ça peut être toute sorte d'information.

Donc voilà à quoi ressemble le type RR. Il s'agit d'un numéro alloué par l'IANA aux entreprises. Donc si vous voulez avoir vos propres types RR, vous pouvez les inclure ici. Et le deuxième champ, c'est un type DGA. Il y aura une allocation avec les données contenues et c'est là que vous pourrez trouver des données, avec une explication, texte en crypté ou texte binaire. Et ensuite, s'il y a des données, on peut les inclure ici, sachant qu'il ne faut pas qu'elles soient trop longues.

Diapo suivante s'il vous plait, c'est la plus importante.

Donc, on a pensé à un prototype pour cela. Et quelle est l'utilisation de cela ?

On a pensé aux domaines IoT. On en a beaucoup parlé, beaucoup entendu parler par rapport aux identifiants persistants et aux différents dispositifs. Donc on pense à une entreprise, appelons là BigCo qui crée des outils IoT. Donc au

titre de l'ancre de persistance, nous donnons une étiquette à cette entreprise, étiquette 12.

Et pour vous donner une idée de ce qu'on peut mettre dans ces informations, pour décrire l'entreprise, on peut donner un certain nombre d'informations : contacts, adresses mails, etc, et décrire le modèle d'outil.

On peut avoir la même chose, et avoir aussi un pointer, ou un firmware, une signature firmware.

Donc ensuite on peut se poser la question : est-ce que j'utilise la bonne version du logiciel ?

On va maintenant passer à la démonstration, et je vais passer la parole à Fernando.

FERNANDO LOPEZ: Bonjour, je vais parler en espagnol.

Bojnour Fernando de l'université nationale de La Plata. Je suis enseignant et chercheur à l'université de La Plata en Argentine.

Une équipe à l'université par l'intermédiaire de Cabase a commencé à travailler sur la création d'une démonstration, d'une démo, une application pour les enregistrements DOA.

Donc au début Cabase a enregistré le domaine persistent.lat, et notre service a configuré toute une série de serveurs, donc deux serveurs qui donnent des registres DOA. C'est une version bêta. Mais ils n'ont aucune modification, c'est simplement une version bêta, et ils mettent en œuvre le DNSSEC.

Pour ce qui concerne les dispositifs, c'est là qu'on a développé la démo, on travaille avec des dispositifs qui s'appellent NodeMCU qui utilise un microcontrôleur à faible coût qui contrôle le wifi qui s'appelle ESP 8266, et on a une antenne qui coûte moins d'1,50USD, et ce sont des programmes disponibles en différentes langues.

Pour mettre en œuvre la démo, ce qu'on a du faire modifier libraire WEP, qui est la bibliothèque qui supporte cet outil. A l'intérieur de cette bibliothèque, on a permis l'envoi et la réception d'une réponse.

Donc la démo on va la couper un peu ; D'abord il fallait configurer le registre. On va sauter l'étape une et trois.

Quand on va lancer il va y avoir une requête par DOA et le serveur va recevoir la réponse, et à l'intérieur de la réponse, il va voir quelle est la version la plus neuve, ou nouvelle du firmware, et une signature du firmware.

Ensuite, s'il y a une version plus nouvelle, il va y avoir une actualisation automatique.

Est-ce qu'on peut retourner s'il vous plait au plein écran ?

Vous voyez ici la photo du dispositif que je vais vous montrer. Et donc c'est la partie qu'on va sauter.

Alors est-ce qu'on peut revenir à l'autre écran s'il vous plait ?

Alors attendez une petite seconde.

À gauche vous allez voir le processus de lancement du dispositif. Le mien, il est connecté par USB à mon ordinateur pour pouvoir le lancer. Et à droite, vous allez voir une capture du trafic DNS et réponse.

En rouge, vous allez voir les requêtes DNS et en bleu réponses avec enregistrement DOA décodé.

Donc la première étape, c'est la consultation. Dans la réponse, on a la description, ensuite le champ avec l'URL, le champ version, un mail de contact et le champ signature.

La partie capture est un peu plus lente que normale pour qu'on puisse voir ces champs. Mais de toute façon, vous pouvez voir qu'on a reçu toutes ces informations. Et l'étape suivante, on va

commencer à télécharger le firmware pour commencer à télécharger.

Ca prend quelques secondes, ensuite ça se ré-initie et ensuite ça commence.

Donc en fonction de la connexion ça peut prendre quelques secondes de plus. Là il est en train de faire l'actualisation.

Alors en attendant, je vais vous raconter la chose suivante, la modification réalisée, elle est mineure pour faire une mise en œuvre. On a modifié 300 lignes, ça a requis des semaines de mises en œuvre, et il n'y a eu qu'une semaine de mise en œuvre.

De l'autre côté vous pouvez voir comment ce dispositif est actualisé, il a été réinitialisé, et il contient donc la nouvelle version 1.0.

ALAIN DURAND: Merci Fernando. Je voulais ajouter quelque chose. Lorsqu'on a essayé de faire cette démo en direct, et lorsqu'on est passé à IPv6 pour organiser cette démo, ça a fonctionné.

Et je voulais remercier les gens de l'université de La Plata, et Albert de l'organisation Cabase qui ont créé cette démo en l'espace de trois semaines.

Donc vous voyez ici ce dispositif dont on parle qui coûte 1,5 dollar.

DAVID CONRAD: Est-ce que vous aviez une question ? Oui, oui, on a 5 minutes pour les questions dans la salle. Et on commence avec Steve qui a une question.

STEVE CROCKER: Non, non, je ne voulais pas vous passer devant.

Alors, l'actualisation a un peu retenu mon attention. Bien sûr, c'est une excellente chose, une actualisation automatique, mais ensuite c'est un problème lorsque vous perdez le contrôle du dispositif. Alors comment vous vous assurez de ne pas perdre des informations lors de l'actualisation ?

FERNANDO LOPEZ: Oui, pour l'actualisation, il y a actualisation uniquement s'il y a une vérification du hash et que cette vérification est valide.

STEVE CROCKER: Oui mais, que se passe-t-il s'il y a un bug à ce niveau-là ?

FERNANDO LOPEZ: Alors il faut que vous mettiez en œuvre une autre solution comme un reset physique, ou quelque chose comme cela.

ALAIN DURAND: Oui, ça n'est pas encore un produit.

STEVE CROCKER: Oui, mais moi j'aime les preuves.

DAVE PISCITELLO: Alors tout d'abord merci beaucoup d'avoir mis en œuvre tout ça, c'est très intéressant. J'adore le fait que vous avez expliqué quelque chose de très complexe, et vous l'avez expliqué de telle manière qu'on peut le mettre en œuvre dans une période de temps très courte.

Est-ce que vous avez pensé, plutôt que de vous concentrer sur le niveau des données, à un niveau objet, pour avoir un enregistrement des données. Parce que si vous le faites, on est en train de rattraper les réseaux zombies.

Donc lorsqu'il y a une infection de fichiers malveillants, il pourrait y avoir un dropper firmware, et ce que ferait ce dispositif, c'est utiliser le DNS pour s'inscrire lui-même et recevoir des instructions.

Donc j'aimerais suggérer que plutôt que de l'appeler DOA ou DTA, appelez-le OBJ pour objet.

Mais merci, c'est réellement impressionnant.

ALAIN DURAND: Si vous permettez que je réponde rapidement.

Oui, on a pensé à ce que vous suggérez, parce qu'on a montré la délégation à une entreprise, ensuite à un modèle d'objet, et on pourrait avoir une délégation au numéro de série actuel. Et on peut déléguer cela afin que ce soit géré par l'objet lui-même et renvoyé au DNSSEC pour validation.

Et dans cette démo, toutes les zones ont été signées par le DNSSEC.

NON IDENTIFIE: Oui, le système du DNS utilise le DNSSEC, ils utilisent ce qu'on appelle le flat space. Donc c'est pas une question pour la persistance du DNS en lui-même, c'est une politique qui a été publiée par l'organisation. Mais l'URL a dû commencer à fonctionner depuis 1990. Donc pourquoi avez-vous choisi de modifier le système DNS alors qu'ils utilisent les racines DNS ?

ALAIN DURAND: Nous ne modifions pas le système, ce que nous avons fait, nous avons créé un nouveau type. Nous n'avons pas changé les serveurs, nous n'avons pas changé les résolveurs, nous n'avons pas changé les milliards de choses DNS qui existent déjà.

Et pour faire cela, nous avons demandé à ce que la mise en œuvre soit faite, et en une semaine nous avions déjà eu 4 mises en œuvre de faites.

Maintenant pour votre second commentaire, pourquoi est-ce que le DOI utilise le DNS ? En fait, ce qu'ils utilisent c'est un proxy. Ils envoient les données à travers http à un proxy.

Comment est-ce qu'on peut éviter le proxy, comment est-ce qu'on peut éviter les questions de vie privée à travers ces proxys en utilisant cette technologie que nous avons utilisée depuis 40 ans. Et la réponse est celle-ci nous le pouvons.

DAVID CONRAD: Bien, y a-t-il d'autres questions ?

JONNE SOININEN: Oui, je voulais rapidement souligner cela. La démo n'est pas seulement pour cet instrument qui fait cette mise à jour, la démo est là pour mettre en œuvre.

Donc ce ne sont pas des obstacles ou des défis par rapport à la capacité de ces instruments. La mise en œuvre est vraiment très simple.

Ce n'est pas une surprise parce que le DNS et les protocoles IP ont été développés à un moment dans l'histoire où le petit outil que vous avez dans votre main aurait demandé beaucoup plus d'espace.

Donc c'est un bon exemple. Nous devrions regarder un peu le modèle de ce que l'on a aujourd'hui, et d'étudier les nouvelles manières avec lesquelles cela peut être utilisé.

ALAIN DURAND: Merci.

DAVID CONRAD: Rick.

RICK LAMB: Oui, c'est fantastique, je suis très heureux de ces mises à jour. Est-ce que vous avez modifié le EPS8266 ?

FERNANDO LOPEZ: Non, on ne vérifie rien avec le DNSSEC.

RICK LAMB: Ce serait vraiment incroyable. Oui, ce serait bien.

FERNANDO LOPEZ: Oui, c'est très important. Pour cette solution ça doit être fait.

ALAIN DURAND: Tout cela a commencé après la réunion LACNIC il y a quelques semaines. Et nous avons eu une bonne discussion avec mon ami de Cabase. Et il nous dit : qu'est-ce qu'on va faire ? Et au lieu de revenir de Montevideo, je suis allé à Buenos Aires, et la journée suivante, ils m'ont dit à l'université de La Plata : est-ce qu'on peut le faire ? On avait trois semaines.

Donc nous avons vraiment eu très, très peu de temps pour nous assurer que cela fonctionnait. Nous avons décrit ce que nous voulions faire, et c'est eux qui l'ont fait.

ASHA HEMRAJANI: Merci, très impressionnant. Et par rapport à la discussion que vous avez déjà eue, je dois dire que, aussi quand il s'agit des mises à jour, nous avons parlé aussi de l'authentification pour qu'on ait les bonnes références. Comment est-ce qu'on pourrait étendre cela à l'authentification de l'instrument, du dispositif ?

ALAIN DURAND: On pourrait authentifier beaucoup de choses. Nous devons penser à d'autres applications qui ont besoin d'identifiants persistants comme celui-là.

Les gens me parlent des références, des données médicales, on pourrait faire quelque chose à ce sujet. C'est quelque chose qui utilise la technologie du DNS, pas pour faire de la cartographie, mais pour envoyer des directions.

Nous avons un identifiant qui pourrait être persistant et qui va démontrer, qui va signaliser tel ou tel objet.

Et donc c'est à vous de décider avec quoi le dispositif va se connecter.

JAY DALEY: Je suis vraiment confus et horrifié avec tout cela.

Pour moi DOA, et on en a parlé au sein de ce groupe, est une technologie qui démontre beaucoup d'erreurs. C'est un modèle qui démontre beaucoup d'erreur. Et c'est peut-être une façon comme ça de régler ces problèmes de technologies, mais les autres dispositifs ne vont pas être réparés, disons, par cela. Alors pourquoi est-ce que l'ICANN fait cela ?

DAVID CONRAD: Oui, une des activités c'est de travailler sur des nouvelles technologies, des identifiants de nouvelles technologies. La DOA est une technologie qui génère de l'intérêt dans beaucoup d'espaces. Une partie de ce projet est de comprendre exactement ce qu'est, ce qu'était le DOA et comment cela fonctionnait au sein du modèle de gouvernance.

Une des choses qu'Alain avait identifié, c'est qu'en faisant cette recherche sur le DOA, nous avons essayé de comprendre que cela n'allait pas changer énormément. La technologie en elle-même est une technologie de nommage. Elle est faite au sein d'un modèle de gouvernance différente. Le modèle de gouvernance est complètement séparé de la technologie et la technologie peut être mise en œuvre au-dessus du DNS.

Donc vous n'avez pas besoin du modèle de gouvernance. Ça faisait partie de la démonstration de cette technologie, et le point que j'essaye de comprendre, quand il s'agit de ce que faisait cette technologie, et donc j'aimerais que nous fassions passer le message à la communauté.

Et avec ça, je pense qu'il est temps de passer à la prochaine présentation.

LEONARD TAN: Léonard au micro. Je présente aujourd'hui le service de nommage Ethereum. Pour ceux qui ne connaissent pas, il s'agit des blockchains. Comme tous les ledgers, toutes les listes, c'est une liste de références numériques, on parle de Paxos, de PBFT. Les chaines, ces chaines que l'on trouve de façon commune, elles sont faciles à établir. Et cela aide à envoyer des textes.

Il y a des transactions, il y a des entrées, et des sorties et de façon à ce que les transactions soient validées, il faut envoyer des informations.

Comme vous le voyez sur la diapositive devant vous, chaque transaction [ascendante] doit être verrouillée par une clef, et ne peut être seulement déverrouillée que si vous avez une clef privée. On ne peut pas ainsi savoir si l'utilisateur a dépensé l'argent deux fois.

Donc on doit pouvoir définir chaque transaction, suivre les règles, et on doit ensuite essayer d'obtenir ce qu'on appelle un hash de chaque block et d'aller au-delà du seuil.

Donc nous pouvons non seulement stocker des données des transactions, mais aussi ajouter, faire des transactions au sein du service de nommage Ethereum.

Ethereum nous permet d'identifier des chaines très longues et dans ce cas-là, les utilisateurs peuvent faire face à des abus.

Nous pouvons utiliser l'ENS pour faire face à d'autres données, tel que Swarm ou les données IPFS. Vous pouvez penser à l'ENS, à un service qui distribue les services de lookup. C'était fait pour pouvoir être aussi mis à jour.

L'architecture interne de l'ENS est en deux éléments. Les registres ENS et les résolveurs. Ainsi, une cartographie des noms peut être répertoriée entre les propriétaires et les résolveurs.

On peut faire trois choses. On peut changer le propriétaire, réassigner le nom à quelqu'un d'autre, ou on peut changer le résolveur, et trois, on peut créer des sous-domaines.

Le rôle des résolveurs, c'est de répondre à des questions sur un nom, par exemple quelle est l'adresse est associée avec un nom, quelle donnée IP est identifiée par rapport à tel nom.

Le registre demande à l'utilisateur quel est tel ou tel résolveur, et le registre répond. Par exemple ici dans ce cas que vous voyez sur l'écran avec Ox1234, l'utilisateur pose la question au résolveur, le résolveur répond.

On a fait un premier lancement durant 8 semaines, et nous avons lancé quelques noms vis-à-vis des utilisateurs. Nous les avons déployés graduellement durant ces huit semaines. À la fin du mois de juillet, 180 000 noms ont été mis aux enchères. Et nous avons vu énormément d'activités. Et une fois que les noms

populaires ont été déployés et ont été pris, on a vu quand même une baisse de trafic. Il s'agit là de 50 millions de dollars US.

Comment cela fonctionne ? Les utilisateurs soumettent une offre, un appel d'offres, et s'ils réussissent, ils obtiennent le nom.

Le projet a été bien accepté par les clients, et nous nous attendons à ce qu'il y ait beaucoup de clients qui vont continuer à utiliser l'ENS dans l'avenir.

Nous avons aussi eu notre premier atelier de travail ENS à Londres, et nous avons eu 27 participants. Durant cet atelier de travail, nous avons couvert beaucoup de questions que nous couvrons ici à l'ICANN, telles que les résolutions de conflit et les sécurités des sous-domaines, et comment intégrer avec les systèmes de DNS tels qu'ils sont aujourd'hui.

Nous avons fait des progrès dernièrement, nous avons pu gérer l'intégration du DNS via le DNSSEC. Vous voyez la chaine de confiance sur l'écran. On commence avec le hashage au départ, et ainsi de suite, comme vous le voyez sur la diapositive.

Donc pour ceux d'entre vous qui connaissent le DNSSEC, vous savez que c'est la même chose, sauf pour la dernière étape. Nous sécurisons des données de textes avec une valeur de l'adresse Ethereum. L'utilisateur soumet une preuve en utilisant les étapes que vous avez vues sur la diapositive, et ainsi Oracle

DNSSEC requiert l'utilisateur d'utiliser une preuve, comme vous le voyez à l'écran devant vous.

Nous avons travaillé sur cela, nous avons mis en place un prototype, et de façon théorique, cela peut être fait par n'importe quel TLD qui soutien le hashing.

Merci. Et restez avec nous, nous vous ferons plus d'annonces très bientôt au sujet de l'ENS.

DAVID CONRAD: Il y a des questions ?

Est-ce que quelqu'un veut poser une question sur cette présentation ?

J'ai une question moi-même. Vous avez utilisé .ETH e je me demande quels sont vos plans pour l'avenir, quand il s'agit des TLD, des noms de domaine de premier niveau et des identifiants que vous allez utiliser pour cela.

LEONARD TAN: Oui, nous comprenons que .ETH est un code de pays à trois lettres pour l'Éthiopie, donc nous savons très bien qu'il n'est pas question d'utiliser celle-là. Nous faisons des tests pour voir si

l'ENS est fonctionnel et ensuite nous verrons comment nous allons poursuivre.

DAVID CONRAD: .ETH c'est un code trois lettres qui n'est pas réservé, donc le fait qu'il s'agit du code pour l'Éthiopie ne s'applique pas, cela ne veut pas dire que cela a été réservé pour l'Éthiopie, surtout si la prochaine série de TLD se poursuit.

JOHN LEVINE: Oui, quand vous parlez de Bitcoin par exemple, qui est très contrôlé en Chine, est-ce que vous savez qui fait ce que l'on appelle le mining pour Ethereum?

LEONARD TAN: D'abord, quand on parle de Bitcoin, vous savez que tous les, ceux qu'on appelle les mineurs vont toujours où il y a de l'incitation. Parce qu'ils répondent aux incitations.

JOHN LEVINE: Si vous rassemblez plus de 50 % de ceux qu'on appelle ces mineurs, ils montent de toute façon.

Au lieu d'argumenter pour voir si c'est possible, je voudrais savoir en fait, est-ce que vous avez une idée de qui sont les

mineurs ? Ou est-ce que vous ne vous souciez pas d'un groupe de mineurs qui pourraient prendre, qui pourraient donc capturer votre blockchain.

LEONARD TAN: Oui, il y a quelque chose qu'on pourrait faire pour que ce soit mieux distribué. Mais quand il s'agit de votre question, notre devoir est de nous assurer que les gens ne se regroupent pas pour faire cela, je ne pense pas que nous pouvons le faire. Nous pouvons essayer, nous ne pouvons pas faire bloc, ce n'est pas possible ça va être trop difficile.

DAVID CONRAD: Y a-t-il d'autres questions ?

PAUL WOUTERS: J'ai une question. Disons que l'IETF reçoit le domaine IETF, et que nous payons, nous faisons notre contribution financière pendant des années, et puis nous oublions de payer. Donc le nom de domaine va être redistribué. Nous allons arriver ensuite à avoir des conflits. Et nous voulons récupérer notre nom de domaine.

LEONARD TAN: Oui, maintenant vous pouvez changer, mais il faut qu'il y ait un consensus, s'il y a 7 développeurs par exemple, il faut qu'il y ait le consensus des 7 développeurs pour pouvoir changer. C'est possible, mais ça va être très difficile à faire.

DAVID CONRAD: Oui, une autre question et ensuite nous allons passer à la prochaine présentation.

JORDI PAILLISSE: Oui, lorsqu'il s'agit du débat sur le minage, les mineurs ne doivent pas forcement passer à travers ce processus. Cela prend une approche différente, ils utilisent les valeurs à l'intérieur du blockchain pour générer un nouveau block. Peut-être que cela devrait être souligné une fois de plus.

DAVID CONRAD: Merci Léonard de cette présentation. On va avancer. Peut-être que Pindar Wong va nous faire la prochaine présentation.

Oui, est-ce qu'on peut changer les diapos à l'écran ?

PINDAR WONG: Merci beaucoup de nous avoir invités. Michael et moi-même sommes volontaires dans le groupe sur le blockchain de

l'internet society. On travaille sur l'évolution de ce que l'on appelle la blockchain.

Il s'agit d'une technologie relativement récente, on ne sait pas encore si ça marche bien, mais ce qui nous intéresse, c'est le développement du système de nommage tel que celui que vous voyez. L'ENS c'est l'un de ces blockchain.

Hier, il y avait 1234 blockchains et actuellement il y en a 1244, donc c'est en perpétuelle évolution, avec des adresses à 34 caractères qui sont aléatoires avec une manière facile d'être gérés en utilisant des noms.

Donc pour comparer les choses de manière générale, il y a de toute évidence quelque chose qui se passe ici qui pourrait impliquer les noms et les gouvernements.

Donc j'aimerais tout d'abord vous remercier de nous avoir invités, et en particulier Michael qui a attiré mon attention là-dessus, sur ce domaine de risque.

Je sais que nous avons commencé cette discussion il y a longtemps, avant que les choses ne se présentent de cette manière.

Aujourd'hui, il s'agit du troisième engagement avec la communauté ICANN, ça fait partie d'un processus où on essaye

de voir quelles sont les opportunités et les risques relatifs à Horizon. Hier on a étendu les systèmes de noms de blockchain, et aujourd'hui on veut voir pourquoi c'est pertinent et si c'est pertinent pour l'ICANN s'agissant de l'évolution.

Donc comme vous le savez, pour l'internet on voudrait que les choses restent en petites pièces, sans trop de distribution. Donc on n'utilise plus maintenant le système de téléphone et la technologie de blockchain est une technologie de pointe.

Et, ce sur quoi j'aimerais insister, qui pourrait intéresser le conseil d'administration et ce comité, c'est que ça pourrait remettre en cause certaines idées toutes faites. Comme par exemple celle d'une racine mondiale et unique.

Mais plus important encore, ça pourrait amener des changements dans la structure de marché qui va modifier tout l'écosystème du DNS. Et ça va modifier également le rythme d'adaptation et d'adoption.

J'aimerais vous donner 4 exemples de l'ENS, dont vous venez d'entendre parler, pour nous l'espérons parler avec le DNS existant, mais on a choisi un autre exemple de ce que pourrait être l'ENS avec une compagnie qu'on appelle Blockstack qui est tout à fait externe au système DNS.

On a déjà un problème de collision de noms avec les systèmes de nom blockchain, mais ce sur quoi j'aimerais me concentrer aussi, c'est qu'hier on s'est penché sur les identifiants décentralisés qui font partie des processus de normalisation qu'on connait.

Par rapport aux risques et opportunités liés à l'Horizon, il pourrait y avoir des systèmes dont on n'est pas caution. Et ici, l'opportunité c'est essayer de faire en sorte que tout le monde soit au courant et joue un rôle de chef de file à cet égard.

Donc on savait que tout le défi ici c'était qu'il fallait gérer internet, ça dépend de combien vous payez. Maintenant il y a des téléconférences sans arrêt, et avant l'ICANN, la gouvernance c'était des traités bilatéraux. On a des exemples très spécifiques où les données peuvent être utilisées de cette manière. Et on doit garantir un internet centralisé avec un internet sûr et vigoureux.

L'important ici c'est que le processus de développement, par exemple Ethereum et le développement qu'on voit aujourd'hui en fait au Mexique, ont un processus de développement qui s'appelle EIP. Le Bitcoin est très semblable, ils ont une conférence également demain à Stanford.

Le travail sur lequel on s'est penché hier, il y a une réunion du TPAC aussi lundi la semaine prochaine.

Blockstack, c'est un processus à part, et ils ont leurs propres documents blancs.

Tout ça pour vous montrer la variété des forums où ce produisent ces discussions. Et peut-être qu'ils ne s'inscrivent pas dans les processus standards qui existent actuellement.

Ils innovent très rapidement.

Le public blockchain, vous aurez entendu parler d'Ethereum et de Bitcoin. Mais on peut voir également les modèles de gouvernances qui peuvent constituer une opportunité pour l'ICANN pour prendre en considération son rôle par rapport à certaines thématiques qu'on a identifiées dans le document.

Sur ce, je vais passer la parole à Michael qui a élaboré une partie du document que vous avez sous les yeux. En tout cas un résumé de ce document.

MICHAEL PALAGE: Merci. L'une des initiatives que l'on essaye de lancer, c'est de sensibiliser par rapport à cette technologie émergente et son impact potentiel sur l'ICANN. L'ICANN devrait être saluée pour sensibiliser, lors de sa première séance à Copenhague.

Maintenant on a un Ethereum ENS. La troisième technologie fondamentale, c'est Blockstack. Dans chacune de ces trois technologies, il y a un impact potentiel sur l'ICANN qui sont inhérentes. Ça peut être lié à un impact en termes d'évolution ou de révolution.

Autre chose que nous avons fait dans ce document, c'est qu'on a essayé de voir ce que font les membres de la communauté en particulier par rapport au « filing » des brevets. L'une des choses qui a retenu mon attention dans ma recherche, c'est que VeriSign a enregistré 3 brevets par rapport aux ancres de confiance du DNS pour des objets qui sont en dehors du DNS. Et également, ils ont fait une référence spécifique en utilisant des blockchains et des ledgers publics.

Donc ça, c'est significatif, ça a lieu, et on n'en est qu'à une analyse initiale par rapport aux enregistrements PTO.

Ensuite il y aura une autre révision pour voir s'il y a une augmentation par rapport à l'utilisation de cette technologie au niveau national.

Ce que notre recherche a également découvert, c'est qu'il y a un certain nombre d'autres foras nationaux qui sont activement impliqués là-dedans. Le W3C, avec d'autres également, l'ISO

T3C0T sur la normalisation de la blockchain et des collègues de l'UIT également avec le SG17 et SG20.

Donc l'objectif de ce document, ça n'est pas d'indiquer à l'ICANN de faire quelque chose en particulier, c'est simplement, et Cherine vous apprécierez cela, Tritia parle toujours de leadership de la pensée, donc l'idée c'est d'assumer un rôle de chef de file en terme de pensées pour l'ICANN par rapport à cette technologie.

On voudrait qu'il y ait des actions qui soient entreprises en amont afin de prévenir tout problème.

Donc, encore une fois, on espère pouvoir publier ce document d'ici la fin du mois.

PINDAR WONG: Oui, il s'agit d'un projet de document, il est là pour donner un cadre, qui est peut-être faux ou pas, on ne sait pas.

Mais en tout cas c'est une tentative pour essayer de montrer la voie et de donner des exemples.

Mais une fois de plus, ces problèmes existent et il y a également de problèmes de ces identifiants persistants.

Et depuis qu'on a commencé, on a cette notion de chain marks, qui sont liées aux marques enregistrées.

Donc la question est de savoir si vous avez des adresses pour des Bitcoin, comment être sûr que cette adresse correspond à ICANN, à Coca Cola ou autre.

Donc, en étant aux avant-postes, on essaye de voir ce qui peut jouer en faveur de l'ICANN, que ce soit en terme de processus ADR et également prendre en considération la confusion qui peut être engendrée dans l'esprit des personnes qui souhaitent enregistrer. Et ça pourrait également distraire certains membres de la communauté ICANN, et les empêcher de participer à d'autres fora tout aussi importants.

MICHAEL PALAGE: Je crois qu'on a encore deux minutes à notre disposition sur les 15 minutes qui nous ont été réservées. Alors… Je pense qu'il y a dans le DNS 180 000 noms enregistrés, si vous le comparez au nombre actuel de gTLD, en 2020, ce sera dans les 50 premiers par rapport aux mille premiers.

Et ensuite, si vous regardez tout le marché des noms de domaine, ça représente environ 55 millions ;

Si vous regardez, par le passé, c'est équivalent à ce qui avait lieu en 98 où il y avait 1,3 million de noms de domaines enregistrés dans le monde pour 35 millions de dollars par an.

Donc il est important parfois de regarder ce qui s'est passé par le passé et de le comparer à ce qui se passe dans l'actualité.

DAVID CONRAD: Wendi ?

WENDY SELTZER: Merci de votre présentation. Vous avez parlé du groupe W3C et des groupes de communauté W3C comme étant une sorte de laboratoire. En fait on est en train d'explorer et de voir s'il y a une piste standard qui peut découler de ce travail du groupe de la communauté du W3C.

Et l'autre groupe de travail se penche lui sur le vocable standard par rapport aux requêtes d'attribution.

Il y a beaucoup d'intérêts et d'impatience par rapport aux couches de données qu'on examine, et lorsqu'il y a un intérêt pour normaliser des composants, nous ça nous intéresse toujours.

PINDAR WONG: Une petite observation. On s'est concentré surtout sur les blockchain, il y a beaucoup de généralisation ici.

Mais ce qu'il faut dire, c'est que la plupart des systèmes sont incomplets parce qu'il y a une couche de sécurité qui fait qu'ils sont incomplets.

Il y a ces jetons qui ont une valeur économique, ça c'est un exemple. Et la valeur économique du jeton affecte les gens lorsqu'ils prennent des décisions. Donc il ne s'agit pas simplement d'un aspect lié à la technologie. Il y a un aspect encouragement économique ou incitation économique.

Mais lorsque cette technologie devient plus systématique, où vous voulez qu'une entreprise prenne cela comme un actif dans un portefeuille, il faut s'assurer que le public, le grand public sait que ce portefeuille lui appartient.

Et on a identifié justement ce domaine, pour savoir comment s'assurer des identifiants d'identités juridiques pour les corporations, pour toutes les blockchains. Parce qu'on ne sait pas de quel blockchain il va s'agir.

Donc c'est à l'ICANN de voir s'il pense, et dans quelle mesure il faudrait s'impliquer dans d'autres fora et quelles seraient les modalités d'engagement, que ce soit des modalités proactives,

réactives ou autre. Si vous pensez que c'est une opportunité, ou bien au contraire une menace.

DAVID CONRAD: Merci, nous allons passer à notre dernière présentation ce soir, et il s'agit d'une présentation de notre président pour près de 24 heures à peu près, donc il s'agit de la présentation de Steve Crocker. Cherine ?

CHERINE CHALABI: Oui, si vous m'excusez, j'aimerais intervenir. Ce que j'ai cru comprendre, c'est que la technologie DNS telle qu'elle existe actuelle, ne va pas survivre, c'est 9a ? Soit elle doit être améliorée, soit remplacée par cette nouvelle technologie. Est-ce que vous êtes d'accord avec cela ?

DAVID CONRAD: Oui, j'ai toujours pensé que les choses changent toujours, qu'il y a toujours un vecteur de changement. Ce vecteur est encore incertain pour moi. Mais il y a toujours un aspect fascinant par rapport au monde blockchain.

Il y a toute une série d'arguments qui montrent que ça évolue, mais il y a toujours un certain nombre de doutes. Parce que je ne fais pas, je ne comprends pas complètement la technologie.

Donc moi, j'encourage les membres de mon équipe à essayer de comprendre la technologie blockchain, à comprendre ses implications, et dans quelle mesure elle va avoir un impact sur l'écosystème ICANN de manière plus générale et dans quelle mesure ça va affecter le système sur lequel l'internet repose.

Oui, vous, que pensez-vous ?

PINDAR WONG: Non, en fait, ces histoires d'échelonnage ne fonctionne pas bien. Nous essayons d'expliquer le protocole Bitcoin. Nous apprenons le protocole. Nous faisons maintenant plus de transactions, nous en sommes à 40 000 transactions par secondes, nous avons deux réseaux qui peuvent procéder à 100 000 transactions et plus.

Nous sommes intéressés à la communauté technologique. La communauté des Bitcoin maintenant est maximaliste. Qu'est-ce qui va en résulter ? Je ne sais pas, mais quelque chose a lieu en ce moment.

Et pour que cette technologie réussisse, il faut qu'elle soit plus facile à utiliser.

Souvent on parle de nommage, mais ça, ça peut être une erreur. Qui sait ? Pour l'instant, il faut que ce soit plus général, plus utilisable.

Le DNS c'est le premier exemple, c'est le plus facile à comprendre. Mais les transactions d'une machine à une autre n'ont pas besoin de DNS. Donc de quoi parlons-nous exactement ?

Si nous assumons qu'il s'agit d'une racine simple, unique, et que c'est définitif, quel système pourrons-nous utiliser ?

Cela veut dire que maintenant, il ne faut pas trop s'engager au niveau du [tack]. Mais nous devons penser que si nous assumons que ce qui se trouve dans l'ADN de l'ICANN peut être changé, c'est important.

Je voudrais donc encourager à ce que tout le monde développe ses propres technologies de chainage de block.

JAY DALEY: Je pense qu'il faut qu'on sépare le DNS du business des affaires des opérateurs de registre.

DAVID CONRAD: D'accord, maintenant, docteur Crocker voulez vous prendre la parole ?

STEVE CROCKER: Si on compare, on voit que cela soulève un sujet, un problème très simple quand on compare la technologie existante et ne pas rajouter des paradigmes nouveaux à travers l'écosystème. Et ce sont des choses très avancées.

Prochaine diapositive.

Ha c'est moi ? Pardon.

Il n'y a rien qui reconnait ma voix sur ce système.

Voilà.

Ce travail est le résultat des conversations que j'ai subies pendant des années.

J'ai eu des entrevues, face à face, avec différents représentants des gouvernements. Et ces personnes parlent de menaces sérieuses, que ce soit le gouvernement US ou l'ICANN s'il y avait donc un changement abrupt, et qu'ils retiraient leurs entrées de la racine. Par exemple les codes de pays, etc. Et que si ces codes disparaissaient, et que la racine renvoyait rien en échange.

Si on imaginait que cela se produisait durant une période où il y aurait pas exemple des tensions politiques, cela les préoccupe.

Donc nous savons qu'il faut qu'on se mette dans des situations où cela ne se produise pas. Mais si cela se produisait, l'impact très lent. Nous aurions 48 h pour le faire. Donc l'effet serait de 2 % de dégradation par heure, au niveau des caches.

Donc la nouvelle, par exemple, de cette menace se propagerait à 10 ou 15 fois la vitesse de la lumière à travers le monde.

Il faudrait donc pouvoir régler le problème, et l'effet serait très différent de ce que des représentants du gouvernement auraient pensé que l'on puisse faire pour résoudre le problème.

Donc si quel que gouvernement que ce soit voulait causer des embarras au gouvernement américain, il pourrait le faire, et il y aurait donc un embarras total et il y aurait un effet désastreux sur la crédibilité de l'ICANN et du gouvernement américain.

Et j'ai bien aussi compris que les gens qui poussent ce sujet comprennent tous ce que j'ai dit. Ce ne sont pas des gens qui sont stupides ou mal éduqués.

Ce problème pourrait devenir une question importante.

Est-ce qu'il serait possible de faire face à cela, pas avec des arguments politiques, mais avec des protections techniques très

puissantes afin qu'il soit impossible, absolument impossible que ce genre de scénario se produise ?

Donc je vais mettre cela en contexte.

Comme je l'ai dit, le scénario cauchemar serait celui : une entrée serait retirée de la racine abruptement. On entre des choses de la racine, très souvent, on a un processus pour le faire. C'est pas que nous ne faisons jamais de changement. Une fois qu'un processus de changement engage les parties affectées, il faut que ces parties soient d'accord. Si ces parties ne sont pas d'accord, les choses ne se produisent pas. Ce n'est pas suffisant. Il y aurait des circonstances où il ne pourrait pas y avoir un accord possible.

Voilà donc les grandes lignes.

Je vais vous faire passer à un autre niveau de détail.

La motivation est celle-ci : est-ce que c'est possible de mettre en place un système qui inclurait un scénario comme celui-ci ? La réponse est oui.

Le concept est basé sur celui-ci. Il est basé sur un système qui ne pourrait pas être falsifié. Nous avons un système comme celui-ci dans le DNSSEC, et ce qu'il se passe c'est que si vous essayez de falsifier le système ou vous obtenez avec une clef, ce système se

verrouille, le système serait assez inopérable. Mais qu'est-ce qu'il se passe dans ce cas-là ? Si le système est inopérable, on ne peut pas faire de changement.

Donc en échange au lieu de faire des changements inappropriés ou de ne pas faire de changements du tout, c'est comme si c'était un échange entre un faux positif ou un vrai positif. Dans ce cas, et comme dans beaucoup d'autres cas dans la vie, il y a une grande différence entre l'impact d'une erreur spécifique ou d'une autre. Dans ce contexte, faire une erreur en faisant un changement inapproprié c'est bien pire que de faire un changement au départ.

On ne sait pas combien de temps ça prendrait, mais on le sait maintenant avec les SLA. Pendant un moment nous avions de la flexibilité, nous savions combien de temps cela prendrait pour faire un changement. Donc cette nouvelle situation fonctionne bien.

C'est un système qui ne peut pas être falsifié. Nos mises à jour courantes ont un certain contrôle, ce qu'on appelle un Split contrôle avec une base de données qui est maintenue par les PTI de l'IANA. Et celui-ci est maintenu par VeriSign, et les communications entre eux. Ce n'est pas impossible à faire ;

La prochaine déclaration est celle-ci : vous pouvez penser à la zone racine comme une division entre des portions très fines, avec une portion à chaque domaine de premier niveau. Quel est l'ensemble des noms de serveurs qui sont associés avec ça ?

Au DNSSEC, nous avons aussi des clefs. Il y a d'autres détails qui sont pertinents, on peut avoir des discussions sur ce qu'on appelle les entrées bleues, mais cela prendrait beaucoup plus de discussions, avec beaucoup plus de détails qui ne seraient pas appropriés durant cette discussion même.

Donc le prochain concept dont j'ai parlé tout à l'heure, c'est qu'aucun changement ne puisse être fait à la portion de TLD de la racine sans qu'il y ait de concurrence d'opérateur. Cela ne dresse pas les pleins potentiels à partir des opérateurs ccTLD et leurs gouvernements. Souvent ceux-ci veulent faire des changements et cela ne se produit pas rapidement ou pas du tout. Et on peut aussi mentionner qu'il y a une partie du système qui est quand même robuste. Il y a aussi des problèmes qui ont émergé dont on pourrait aussi parler.

Mais, si vous y pensez, on parle d'un jeton hardware, si vous voulez, un dispositif qu'on pourrait donner à un opérateur TLD, ils doivent utiliser ces dispositifs pour authentifier et autoriser un changement potentiel. S'ils ne le font pas, le changement ne peut pas avoir lieu.

Comment est-ce qu'ils obtiennent ça en tout premier lieu et comment est-ce qu'on fait l'association entre la demande et le dispositif. C'est un processus différent qui demande de régler cette question, du fait qu'un changement peut se produire ou ne pas produire. C'est un processus laborieux, et nous avons des cérémonies de clefs et d'autres processus qui sont similaires. Beaucoup de personnes se mettent d'accord sur cela, et ces personnes sont indépendantes, et ainsi il n'y a pas de collusion et il y a moins de pression, et le processus est ainsi un peu lent, plus délibéré et plus raisonnable.

Voilà une solution que l'on pourrait utiliser, ce genre de processus lent.

Mais si vous voulez retirer quelque chose de quelqu'un en cas d'hostilité, et que vous devez [redécerner] un nom de domaine.

Donc voilà une autre chose que l'on doit garder à l'esprit, c'est que tout le monde ne peut pas être capable de faire tout cela, tout le monde ne peut pas faire tout cela d'un seul coup. Nous n'avons seulement que 1500 opérateurs de TLD en ce moment, 10 d'entre eux seront prêts aujourd'hui et les autres prendront un peu plus de temps.

Les derniers prendront certainement de 2 ans à 10 ans. Quoi qu'il en soit, c'est un processus de transition.

Il faut toujours être prêt à opérer au sein du système courant et du nouveau système. Il n'y a pas de problème de ce côté-là.

On pouvait penser à refaire le système complètement, et avoir tout de même un dispositif pour tous les opérateurs TLD qui soit là à disposition, et ceux qui seront prêts à les utiliser pourront les obtenir et commencer la démarche.

Voilà donc sur l'écran une schématique sur le processus de mise à jour de la zone racine courante. Comme vous le voyez sur l'écran, vous avez le PTI qui valide la demande et qui vous dit si c'est ok, qui l'envoie à VeriSign qui est la boite que vous voyez sur l'écran en bas. Et là il se passe deux choses, ils font une correction de la base de données et ils génèrent une zone. Et puis ensuite cela passe au processus de distribution, deux fois pas jour. Et une nouvelle version de la zone est introduite. Voilà donc le processus de mise à jour aujourd'hui. Et les changements dont nous parlons sont sur la prochaine diapositive.

Comme vous le voyez, il faut rassembler cette colonne que vous voyez au milieu dans un seul système qui serait compact, et qui ne pourrait pas être falsifié pour que le protocole soit plus robuste et que la connexion se fasse entre eux.

Prochaine diapositive.

Pour répéter, il y aura donc deux sortes de transactions, les transactions ordinaires pour les changements réguliers, et pour tout ce qui est données NS et le DNS key. Cela passera par une piste rapide, l'opérateur dira je veux ce changement, et voilà donc mon autorisation pour ce fait, et ce changement peut-être approuvé ou non approuvé, mais il ne peut pas être falsifié. Et le changement est fait ou non.

Les changements les plus importants sont les changements de contrôle qui demandent un processus plus élaboré.

Prochaine diapositive.

Voilà encore une fois un autre diagramme pour montrer ce qu'un changement ordinaire pourrait donner. Et ensuite voilà une diapositive sur les changements importants.

Je voulais expliquer les choses ainsi. Le grand ovale que vous voyez en haut de la diapositive représenterait disons une table de conférence et voilà en dessous tous les processus qui sont associés. C'est un petit peu comme nous faisons notre cérémonie de clef avec les représentants de notre communauté.

Prochaine diapositive.

Et là bon, je résume un peu les choses que j'ai déjà dites sur ces diapositives. Donc l'organe de supervision serait composé de représentants de confiance.

Prochaine diapositive.

Bon, si on voulait explorer ceci, il serait de mettre en place un concept qui soit bien documenté. Nous devrions diviser le travail sur trois pistes parallèles. Nous déterminerions ainsi comment est le processus, nous pourrions construire des prototypes, des interactions entre les opérateurs de TLD et le système, et ensuite nous pourrions construire un prototype du système en lui-même et de comment il va fonctionner. Donc ces trois étapes pourraient être faites dans n'importe quel ordre.

Prochaine diapositive. Voilà. Prochaine diapositive.

Voilà c'est ça dont je vous parlais. Voilà donc le concept. J'y travaille depuis longtemps, depuis plusieurs années d'ailleurs. Je ne me rappelle plus vraiment quand j'ai commencé à travailler sur cela. J'ai arrêté d'en parler complètement, j'avais mis ça de côté quand le processus de la transition a commencé parce que je pensais que ce serait une cause de distraction, et cela causerait beaucoup de confusion.

La transition est maintenant terminée et nous y voilà une fois de plus.

Merci.

DAVID CONRAD: Avant de passer aux questions, je dois vous dire que mon équipe va publier un fait pour deux sortes de changements pour la gestion du mécanisme de la zone racine. Nous espérons ainsi améliorer les choses. Nous voulons avoir une approche révolutionnaire pour pouvoir restructurer la façon dont nous faisons les choses. Et nous avons pensé à incorporer cela dans l'approche révolutionnaire dont nous parlions tout à l'heure.

Y a-t-il des questions à ce sujet ? Il nous reste que deux minutes pour les questions, à moins que les gens ne veulent pas aller au cocktail qui va suivre, et ça je crois que Kathy n'en serait pas très contente.

Rod ? Vous voulez la parole ?

ROD RASMUSSEN: Je pense que tout cela est… Vous avez parlé d'une approche intéressante, cette gestion de la zone racine est un sujet intéressant. Le point brand TLD, le point marque TLD pourrait être très intéressé. Mais pourquoi est-ce qu'on va s'arrêter à la racine ?

STEVE CROCKER: Oui, précisément, la même technologie est applicable à tous les niveaux. Point à la ligne.

DAVE PISCITELLO: Le modèle de menaces est celui-ci : les gens pensent que quelque chose va disons casser. Ce que je voudrais voir, un modèle de menace comme ça et une analyse de risque pour voir quels seraient les résultats finaux des changements et quelles sont les menaces que nous pourrions atténuer, que nous ne faisons pas aujourd'hui. Je ne vois pas la menace aussi logique que ça, quand on parlait des États-Unis qui nous retiraient notre délégation.

STEVE CROCKER: Si vous êtes assis près du centre du monde, comme vous et moi, on pense que c'est tout à fait ridicule et que ça ne va pas se produire, et que personne ne devrait être inquiété par ce genre de changement. Et si vous vous éloignez un petit peu, alors vous vous dite : ho lalla il y a un gros risque, toutes les économies du monde vont tomber à l'eau du jour au lendemain. Ça c'est le modèle de menace.

DAVID CONRAD: Dernière question oui ?

LARS-JOHAN LIMAN: Est-ce que ça peut vouloir dire qu'une personne dit : je veux faire ce changement et non… alors est-ce que ça permet de prévenir un refus de service ?

STEVE CROCKER: Non. J'ai eu une conversation intéressante il y a quelques années avec l'un des principaux opérateurs de TLD. Et je lui ai demandé : combien de temps ça devrait prendre pour apporter une transformation à l'opération de votre nouveau serveur de nom. Et il a dit maximum 48 heures. Par rapport à quelques secondes. Donc je le lui ai demandé, et combien de temps est-ce que vous prévoyez pour cela ? Il m'a dit 6 à 8 semaines.

Pourquoi ? Parce qu'à l'époque où on a parlé, il faisait la demande et il n'était pas sûr que ça se produise. Maintenant la situation est bien meilleure.

Toutefois, j'ai l'impression que les opérateurs de TLD vont faire des changements dans leur configuration de serveurs de noms et qu'ils ne sont pas dans une situation où ils peuvent le faire de manière instantanée, qu'ils font une demande et qu'il y a un échelonnage instantané.

Donc en fait, le fait que ça ne se produise pas, c'est parce que ça ne se produit pas dans la minute suivante, mais ça prend un peu plus de temps par rapport à des négatifs absolus.

LARS-JOHAN LIMAN: Oui, mon idée c'était un déni de service pour des raisons politiques.

STEVE CROCKER: Oui. Ça peut se produire au niveau politique.

DAVID CONRAD: Au point divers, toute personne intéressée par le cocktail devrait s'orienter vers l'entrée principale, et on aura des bus qui vont nous emmener sur un pont qui va nous permettre d'observer un très beau bâtiment qui est très connu.

Merci à tous, et on se retrouve à Puerto Rico.

Merci.

[FIN DE LA TRANSCRIPTION]