

---

BUENOS AIRES — Réunions des boursiers après-midi

Mercredi 24 juin 2015 — 17h30 à 19h00

ICANN – Buenos Aires, Argentine

JANICE DOUMA LANGE : ... Et je ne peux pas croire qu'avec mon zéaiement j'ai réellement dit cela et m'en suis sortie. Nous allons voir passer différents membres de l'équipe SSR du personnel de l'ICANN. Ils ont tous à des degrés divers une expérience sur différents aspects de la sécurité, mais ce sont aussi tous des généralistes et ils peuvent donc répondre à toutes vos questions.

Steve, je vais prendre l'initiative et vous donner la parole en premier. Steve Conte, que certains d'entre vous connaissent peut-être de l'ISOC [gloire]. Mais avant l'ISOC, il faisait partie de l'ICANN et il vient de rentrer à la maison. Bienvenue !

STEVE CONTE : Merci. J'aime à l'appeler « MyCANN » s'il vous plaît. Je n'ai personne de mon autre équipe ici. Ils m'ont laissé planté là, c'est pour ça que je me suis pris [de la bière]. John, je pense que vous avez vu John Crain parler à la séance des nouveaux venus, exact ? Je ne veux donc pas répéter trop de choses sur ce que fait le SSR. Je vais récapituler rapidement, et puis je vais vous laisser la parole et avoir un dialogue sur ce qui est important pour vous les gars en termes de sécurité, stabilité — vous voyez, je ne peux pas le prononcer et pourtant c'est

---

*Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.*

---

mon département — et de la résilience. Je le rate à tous les coups. Des munitions pour vous.

Nous examinons la question dans une perspective que je vais appeler de la SSR, car je peux dire ça beaucoup plus rapidement et plus facilement. Nous examinons la SSR en ce qu'elle a trait à l'Internet dans son ensemble sur le système de noms de domaine, sur l'adressage IP unique et des choses comme ça. Nous ne sommes pas nécessairement concernés — professionnels concernés — par le spam et des choses comme ça. De toute évidence, nous sommes tous personnellement concernés parce que je reçois autant de spam que vous les gars et le déteste tout autant. Mais le spam n'affecte pas vraiment la stabilité ou la résilience de l'Internet dans son ensemble.

Donc, nous examinons les choses en nous posant la question de comment maintenir un système unifié et unique de DNS dans le monde et comment ne pas le fragmenter, parce qu'un DNS fragmenté risque de compromettre la stabilité de l'Internet, parce que si vous vous attendez à aller sur un site web dans un Internet, si le système de noms de domaine est fragmenté, vous risquez peut-être d'aller sur un autre site web ou chez un hôte différent. Donc, nous vérifions les choses comme ça.

John a probablement mentionné notre travail avec les représentants de la loi et les services de sécurité publique. Nous aidons à enquêter sur les logiciels malveillants. Nous travaillons avec les forces policières du monde entier pour les aider à comprendre ce que le DNS fait et les outils qu'ils peuvent utiliser pour aider à instruire un dossier contre les

---

méchants qui font des choses et abusent du DNS pour faire de mauvaises choses via des logiciels malveillants ou les réseaux de zombies ou enregistrements malveillants, des choses comme ça.

Nous ne sommes pas les flics de l'Internet. John peut dire le contraire, mais non, pas nous. Nous ne lançons personnellement aucune recherche. Nous aidons lorsqu'on nous demande d'aider. Particulièrement lorsque nous travaillons avec la police ou des organismes politiques, nous voulons être très clair sur le fait que nous sommes là pour les aider, pour les aider à comprendre ce qu'est le DNS ou les identificateurs uniques et quels sont les outils qu'ils peuvent utiliser pour faire tomber les méchants, comme s'ils étaient des flics dans la rue et qu'ils traquaient [en cherchant des indices] quelqu'un ayant volé une voiture. Ils ont besoin d'accumuler des preuves pour qu'arriver devant un juge, ils puissent avoir les éléments pour faire enfermer les méchants.

Donc, nous faisons la même chose avec eux en les aidant à comprendre à quoi ressemble le paysage numérique et comment ils peuvent trouver des preuves pour pouvoir arrêter les méchants.

Nous faisons de la formation. J'ai rencontré [Naveed] ici au travers de diverses formations. Nous formons sur le DNS. Nous formons, comme je viens de le dire, les représentants de la loi, locaux ou régionaux. Nous formons au DNSSEC et nous allons dans le monde entier faire toutes sortes de formations principalement pour les ccTLD qui sont dans des régions émergentes pour les aider à développer cette

---

compétence localement. S'il y a un besoin et que nous pouvons y aller, nous sommes heureux d'y aller et d'aider.

Je ne sais pas vraiment quoi dire, donc je vais ouvrir la parole et vous laisser, vous les gars, me parler et voir s'il y a quelque chose sur lequel je n'ai pas été clair ou John n'a pas été clair, ou maintenant que vous avez assisté à une réunion de l'ICANN pour la première semaine, ce que signifie XYZ ou autre chose ? Je tiens un peu à conserver cela comme un échange, une conversation pour aujourd'hui. Et je vais prendre une gorgée de bière pendant que vous parlez. Naveed ?

NAVEED HAQ :

Naveed du Pakistan. J'ai une question de déploiement, plus précisément de la perspective des DNSSEC, puisque les gens seraient — je vois que [inaudible] d'avoir cela. Les domaines ne sont pas signés en tant — il y a eu récemment une statistique sur le nombre de domaines qui sont signés et tout.

Les gens disent, comme, combien d'attaques il y a eu dans les 20 dernières années sur le DNSSEC qui pourraient les obliger à utiliser ou adopter le DNSSEC. Cela ressemble, sans être exactement la même chose, mais disons que — les avions peuvent s'écraser, prenons un parachute à bord pour chaque passager. Mais les avions ne se crashent pas récemment. Qu'en pensez-vous ? Comment répondre à ces gens qui arrivent avec de telles questions ? Leur point de vue se défend. Merci.

---

STEVE CONTE :

C'est une question intéressante. Le DNSSEC est, je crois, mal nommé, d'abord. Ce n'est pas tant de la sécurité du DNS que de l'authentification du DNS. Lorsque vous utilisez le protocole DNSSEC, vous n'êtes pas vraiment en train de chiffrer un paquet ou la conversation entre les deux serveurs DNS. Vous authentifiez le fait que la question que vous avez posée à l'hôte et la réponse qui vous revient proviennent effectivement de cet hôte.

À cause de cela, il a été très difficile de mettre le DNSSEC sur le marché parce qu'il n'y a vraiment aucune valeur ni aucun retour. Oh, notre personne chargée du DNSSEC est ici !

Il n'y a que très peu de valeur et de retour pour la personne qui implémenterait le DNSSEC. Comment peuvent-ils faire payer les clients ? Ils ne peuvent pas vraiment le faire. Il n'y a vraiment rien à leur refacturer, car tout ce qu'il fait est d'authentifier que la réponse est venue de l'hôte dont vous pensiez qu'il répondrait ou d'où elle doit venir.

Donc, même si nous avons le DNSSEC — et Rick, je vous permets de m'interrompre si je dis une bêtise. Vous pouvez me corriger. Plus nous avons de DNSSEC, mieux c'est. Mais cela ne sera pas vraiment mieux avant que nous ayons des applications qui sont au courant de l'existence du DNSSEC. Ainsi, lorsque votre navigateur est conscient du protocole DNSSEC, l'utilise, recherche les drapeaux spéciaux DNSSEC et vous indique en tant qu'utilisateur, « n'y allez pas ». « C'est authentifié », « Hey, il n'est pas authentifié », « c'est à vous de choisir

---

d'y aller ou pas.» Alors, il commencera à s'implanter et deviendra encore plus précieux pour l'utilisateur final.

NAVEED HAQ :

Alors la question est de savoir comment [inaudible] structure DNS actuelle peut avoir de telles attaques? À quelle fréquence surviennent-elles? Je veux dire, nous n'avons pas de statistiques qui appuient cet argument. Chaque — moitié du DNS n'est pas sécurisée, donc faisons-le. Ou même 10 %. Alors, nous ne l'avons pas. Je veux dire, c'est quelque chose qui est — ne permet pas aux gens d'adopter le DNSSEC. Il faut faire quelque chose par rapport à cette situation.

STEVE CONTE :

Ouais, il y a deux volets. Je suis d'accord avec vous. Je vais vous présenter dans un instant Rick Lamb, à qui je viens juste d'être présenté. Rick Lamb, tout le monde.

Il y a deux volets, car la façon dont je vois le déploiement et l'implémentation du DNSSEC, c'est la question, puis-je obtenir ma mère qu'elle signe la zone sans vraiment comprendre ce que cela signifie? Je pense que c'est vraiment le niveau auquel nous devons agir qui fait que lorsque vous enregistrez un nom de domaine et que le DNSSEC en fait simplement partie, vous dites « d'accord, je vais générer une clé, saisir une "phrase de passe", bla-bla-bla, et maintenant ma mère a une zone signée ». Quand ma mère aura une zone signée, Rick aura fait son travail.

---

Ouais, je sais qu'il reste encore à faire. En tout cas, Rick fait partie de notre équipe. Il est notre expert DNSSEC. Je ne voulais pas le dire trop vite, parce que cela semblerait bizarre. Mais il pourra peut-être répondre à vos questions un peu mieux que je ne pourrais le faire.

RICK LAMB :

Ouais. Allez-y et posez-moi des questions. Je suis sûr que Steve a déjà fait un assez bon travail pour couvrir ce genre de choses. Une chose que je voudrais dire, et s'il l'a déjà couverte, il vous suffira de lever la main. Pour moi, le DNSSEC n'est pas uniquement la signature des zones. Il en a déjà parlé. Oh, vous avez une question. OK, c'est bon.

Naveed, je pense que votre question était que sans quelques statistiques, nous ne savons pas où nous en sommes, ok ?

NAVEED HAQ :

Le point est que nous devons convaincre les gens de la vulnérabilité du DNS sans sécurité. Il n'a pas l'air d'être vulnérable. Je veux dire, les attaques ne se produisent pas si souvent. Pour les banques, nous avons un système bancaire, nous avons tous les systèmes financiers, de l'e-gouvernement. Toutes choses qui vont « e ». Nous avons besoin de trouver quelque chose pour convaincre les gens d'adopter cela. Voilà ce que je voulais dire.

RICK LAMB :

Vous avez absolument raison, Naveed. Vous connaissez Naveed. C'est un professeur et il connaît très bien ce genre de choses. Il marque un

---

point, parfait, vraiment parfait. Vous pensez, « Où est la baguette avec laquelle nous pouvons taper sur les gens pour leur dire que c'est la raison pour laquelle vous avez besoin du DNSSEC. »

Malheureusement, c'est une question du genre la poule et l'œuf. Il est très difficile de convaincre les gens que le DNSSEC a une quelconque valeur tant que le DNSSEC n'a pas une masse critique déployée. Exactement comme Steve l'a dit. Jusqu'à ce que sa mère ait obtenu le déploiement du DNSSEC — en fait, plus important encore que le site web de la banque de maman ait déployé le DNSSEC. En attendant que cela arrive, ça n'a pas beaucoup de valeur.

Le revers de la médaille, — la bonne nouvelle — c'est qu'à cause d'efforts comme ceux de Google, environ 25 % des utilisateurs finaux dans le monde sont assis derrière quelque chose qui fait de la validation, utilise le DNSSEC.

Donc, la seule partie de l'ensemble que nous avons réellement manqué à ce point c'est les gens qui possèdent des sites web. Ils doivent déployer le DNSSEC. Une fois qu'ils le feront, nous aurons réussi.

Pour moi, c'est ce point de pression qui s'étend, s'étend et s'étend. De nombreux TLD ont déployé le DNSSEC. DNSSEC est déployé à la racine. Nous avons ces résolveurs. Peut-être, et je l'espère, vous apprendrez ce que c'est cette semaine. Mais les résolveurs, ces choses qui vérifient les noms pour vous, c'est ça qui fait la validation. Comme je l'ai dit, environ 25 % des gens sont assis derrière cela. Mais il n'y a rien à voir. Aucun des sites web ne le fait.

---

Je pense donc que, pour répondre à votre question, ce dont nous avons besoin — une chose est de montrer les avantages d’avoir DNSSEC versus ne pas l’avoir. Je qualifierais cela de crainte, incertitude et doute. C’est un terme que les gens utilisent FUD (crainte, incertitude et doute).

Un excellent moyen de vendre le DNSSEC est de dire, « Voici ce qui se produit si vous ne l’avez pas. » Et il y a quelques sites qui le font cela — je devrais vous envoyer les liens — qui montrent, « voici ce qui se produit si vous n’utilisez pas le DNSSEC. »

Mais pour la plupart, parce que tellement peu de sites web l’ont, il n’y a pas d’information. Pour moi, la chose la plus importante ici est que c’est formidable que le DNSSEC ne soit pas déployé. Nous avons maintenant une occasion non seulement d’apprendre, mais de faire des erreurs. Nous avons eu beaucoup de chance que le gentleman de dot-ke du Kenya, ils ont eu un problème il y a quelques semaines et il ne voulait pas dire à tout le monde — le monde — qu’il avait totalement raté, mais c’est très précieux. Cette information est très précieuse. Nous l’avons convaincu que nous voulions savoir ce qu’il avait appris pendant que nous déployons le DNSSEC.

Dont, la première chose est que, puisqu’il n’est pas pleinement déployé partout, nous avons la chance effectivement de bien le faire fonctionner. Mais l’aspect le plus important est que c’est une occasion pour tous les entrepreneurs dans cet espace. C’est l’une de ces choses-là où ça se passe, c’est ce qui se passe, ça se passe. Le DNSSEC

---

est [inaudible] technologie, comme ils disent. C'est un bébé. Il est prêt à naître.

Si vous êtes un businessman ou que vous voyez des opportunités, vous voyez que ça se produit, vous pouvez commencer à développer ces idées maintenant. Je ne sais pas. Déposer des brevets, faire tout ce que vous faites. Proposez de nouvelles idées qui vont être basées sur ce principe.

Aux États-Unis, nous avons notre réseau électrique, notre réseau d'alimentation. Il y a tout un effort de diverses sociétés aux États-Unis qui gèrent le réseau électrique qui disent : « Nous allons utiliser le DNSSEC pour distribuer des informations de configuration dans tous vos compteurs, vos petits compteurs, vos compteurs électriques, partout. »

Personnellement, c'est effrayant. L'Internet, l'électricité ? Oh, mon Dieu. Imaginez juste quelque chose qui pourrait vraiment péter ici. Néanmoins, il y a beaucoup d'efforts comme ceux-là qui se font en coulisses, et c'est pour moi une occasion de frapper et de bien le faire.

Et chaque fois que je donne le cours de formation dans différents pays, mon plus grand truc c'est — j'habite dans la Silicon Valley ou près de la Silicon Valley. Je suis écoeuré de voir que le nouveau truc sort toujours de là. Allez ! Ça n'a pas besoin de sortir de là-bas. Ça peut venir de n'importe où. S'il vous plaît, quelque chose d'ailleurs. Je suis fatigué de voir toujours le même gars qui fait ça.

---

Je vois le DNSSEC comme l'une de ces choses pour lesquelles tout le monde n'est pas complètement prêt, mais parce que nous avons les gouvernements et nous avons cet élan, à un certain moment ça passera. Si vous y êtes en même temps, c'est une grande opportunité.

D'autres questions ? Il est le premier, d'accord.

HOMME NON IDENTIFIÉ :

Bonjour à tous. Je vais parler en espagnol. Vous m'entendez bien ? Test. Je vais vous parler de mon expérience au Venezuela. Je suis [inaudible] du Venezuela.

Au Venezuela, nous avons eu l'appui de [inaudible] pour créer des séances de formation sur les concepts et les structures pour le développement de [RPKI], et également des ateliers au niveau IPv6, de manière à faciliter l'adoption de ce projet [dans notre] pays.

Ç'a été très utile. Ça a été coordonné avec le secteur public pour créer ces compétences, et aussi avec les institutions au sein de l'écosystème Internet dans notre pays.

Ma question est de savoir comment l'ICANN peut contribuer à ce phénomène ? Il serait très utile de créer ces séances de formations auprès du secteur qui n'ont peut-être pas une influence telle que le secteur public et le milieu universitaire auquel j'appartiens. C'est tellement nécessaire dans les universités. C'est ma question ou mon doute.

---

RICK LAMB :

Merci beaucoup de votre question. C'est une parfaite question parce que, en fait, c'est ce que notre équipe fait énormément. Nous offrons une formation gratuite, particulièrement sur le DNS et le DNSSEC.

Tout ce que vous avez à faire c'est de demander. Et quand je dis demander, c'est nous envoyer un e-mail, littéralement. Nous voudrions voir au moins peut-être 16 personnes dans la salle pour que cela en vaille la peine. Nous allons essayer de nous organiser pour ne pas envoyer un Américain stupide. Peut-être quelqu'un qui peut parler espagnol serait plus efficace. Il suffit de demander. Nous aimons faire ça. Peut-être comme vous pouvez l'entendre de ma bouche ici, il ne s'agit pas seulement du DNS et du DNSSEC. Lorsque nous aurons ces formations — et je suis tout ému à ce sujet, donc je m'excuse.

Mais vous réunissez ce groupe de personnes dans une salle et vous apprenez à vous connaître les uns les autres. Donc, différentes personnes de l'industrie de votre région, ville ou région apprennent à se connaître.

Et ces relations peuvent parfois durer éternellement. Et c'est là la valeur. Oubliez ça — je veux dire, la technologie est bonne et nous vous montrons comment la faire, sur place. C'est entièrement en mettant les mains dans le cambouis. À la fin, vous savez comment le faire. J'ai même donné aux gens des cartes à puce et de l'équipement. Passons.

Mais ce sont ces relations, finalement dont je pense qu'elles sont : « ouah, je viens de faire une bonne action. » Je ne sais pas. Est-ce que cela répond à votre question ? OK. Intervenez, s'il vous plaît.

---

[STEVE CONTE] : Juste pour compléter, parlez absolument à n'importe quel membre de notre équipe, mais une meilleure façon de faire passer le message dans la région est de parler à nos directeurs régionaux. Nous avons Rodrigo ici. Nous avons Albert ici. Ce sont les personnes auprès desquelles nous voudrions que vous vous rendiez pour quand vous avez une demande de formation hors de la seule portée de l'université. Ils peuvent essayer d'attirer plus de personnes et cela justifie davantage notre raison de venir dans cette région ou dans cette ville et faire de la formation. Je suis d'accord avec Rick, mais veuillez faire le premier pas vers nos représentants régionaux.

En fait, je crois que nous avons une file d'attente, à moins qu'il s'agisse d'un suivi direct. Est-ce directement lié à ça ? Alors, allez-y. Allez-y.

HOMME NON IDENTIFIÉ : Je suis [Ricardo] de la République dominicaine. Je suis un boursier de la Société Internet. Je ne veux pas faire une question sur le DNSSEC, mais sur quelque chose d'autre, donc excusez-moi.

[STEVE CONTE] : Votre question est-elle directement liée à la formation ou avez-vous une autre question ?

HOMME NON IDENTIFIÉ : C'est lié à certaines séances auxquelles j'ai assisté aujourd'hui.

[STEVE CONTE] : OK. Alors, nous avons une file d'attente. Excusez-moi. Je vais vous laisser attendre dans la file d'attente. L'autre chose, en ce qui concerne la formation, je pense que nous avons une question ici, là, là, et c'est ici que nous allons maintenant. Nous avons un programme de formation en ligne. Je suis sûr que quelqu'un vous a parlé de [learn.icann.org](http://learn.icann.org). Nous cherchons à y contribuer aussi. Ce n'est pas — ce ne sera jamais...

[FIN DE LA TRANSCRIPTION]