MARRAKECH – Séances des boursiers de l'après-midi
Mercredi 9 mars 2016 – 18h00 à 19h30 WET
ICANN55 | Marrakech, Maroc

HOMME NON IDENTIFIÉ : Séances des boursiers de l'après-midi, [tech Alex] [inaudible].

FEMME NON IDENTIFIÉE : Bonjour à tous. Ouaouh ! Tout le monde est endormi. Regardez un peu. Vous vous êtes réveillés ? Personne ne dort plus maintenant. Notre après midi sera un peu spécial parce que les bus pour le gala partent à 19h00. Nous essaierons donc de donner du temps à nos orateurs. La dernière réunion avant nous a eu un peu de retard. Et même si nous avons parlé fort à l'extérieur de la salle, ils ne se sont même pas rendus compte... Qu'allons-nous faire ? En tout cas, ce matin c'est nous qui avons été en retard, alors ça a été notre punition.

Merci á tous d'être ici. J'espère que vous aurez tous eu une bonne journée. Demain matin, nous aurons l'occasion de passer en revue notre semaine d'activités. En général, nous essayons d'utiliser ces sessions de l'après-midi pour analyser ce que l'on a fait pendant la semaine, mais il y a eu tellement d'orateurs

qu'on n'a pas pu le faire. Je voulais tout simplement que vous sachiez que nous aurons cette chance demain.

Nos orateurs de cet après-midi seront, Steve Conte et John Crain, du personnel de l'ICANN. Ce sont deux de mes collègues et ils sont là pour nous adresser la parole. De quoi allez-vous nous parler, Messieurs ?

STEVE CONTE : Je ne sais pas encore.

FEMME NON IDENTIFIÉE : OK. Je vous ai dit que vous deviez vous préparer au moins dix minutes à l'avance, alors allez-y.

STEVE CONTE : Combien de temps avons-nous parce que je sais que vous pouvez faire un téléchargement aussi, non ?

FEMME NON IDENTIFIÉE : Oui, je veux leur donner environ cinq ou dix minutes avant 19h00 pour qu'ils aient un peu de temps. Il y a d'autres navettes, soit dit en passant. Ce n'est pas la seule navette. La première navette part à 19h00, alors je veux vous libérer avant 19h00. La séance sera clôturée à 18h20 environ. Nous voulons vous donner du temps pour les questions.

JOHN CRAIN : Bon, eh bien, on dirait normalement que nous sommes entre vous et la bière, mais j'ai entendu qu'il n'y aura pas de boissons, alors nous sommes entre vous et l'eau, ce qui est bien, car je suis convaincu que le repas sera génial. Combien parmi vous sont des boursiers pour la première fois ? Combien parmi vous m'ont vu prendre la parole auparavant ? Très bien, alors je ne vais pas passer les diapos.

Je suis le directeur de la sécurité, la stabilité et la résilience de l'ICANN. Je dirige un petit groupe, auquel Steve appartient. Nous nous occupons de la sécurité des systèmes d'identificateurs, du système de noms de domaine, du routage, etc.

Nous n'avons pas beaucoup de temps, alors je passerai directement aux questions. Qui a des questions à poser sur l'Internet ou sur les identificateurs de sécurité, sur la sécurité la stabilité ou la résilience, ou peut-être sur d'autres questions, comme par exemple nos programmes de formation ? Notre groupe organise un grand nombre de programmes de formation et fait également beaucoup de recherches. On peut s'asseoir ici et passer les diapos, mais je me demande, avez-vous des questions pour nous ? Je vais commencer avec la demoiselle qui est là. Vous voulez utiliser ce micro ?

FEMME NON IDENTIFIÉE : [inaudible] [Tajani]. Vous pouvez commencer par nous dire quels sont les aspects de la sécurité concernant IPv4 et IPv6, peut-être ? Comme identificateurs, comme ressources ?

JOHN CRAIN : Alors IPv6... en fait nous ne faisons pas grand-chose là-dessus en ce moment. Une des questions que nous avons abordées par le passé c'était de nous assurer qu'IPv6 était déployable. Quand on regarde du côté de l'ICANN, et si je veux utiliser IPv6 dans le DNS, par exemple, parce que le DNS s'occupe de traduire les noms, pouvez-vous réellement faire cela ? Si je suis un utilisateur final, puis-je réellement mettre mon quad-As, mes adresses IP dans le DNS ? Si vous regardez les bureaux d'enregistrement, pour la plupart, vous pouvez le faire maintenant.

Voilà donc deux choses que nous examinons. On a analysé si on pouvait mettre quad-As dans la zone racine - et cela il y a quelques années – et bien sûr, on l'a fait – quel est l'effet ? Quelle sera la conséquence de changer la taille de la zone racine, qu'est-ce qu'un fichier DNS pour les TLD pour l'Internet ? Quelle en sera la conséquence ? Nous nous occupons de choses de ce genre. Nous regardons la réalité et nous nous disons : « Eh bien, comment cela va changer les choses ? »

Si vous regardez IPv4 ou IPv6, il y a des points communs. Il y a deux problèmes intéressants à l'heure actuelle. L'un d'eux est le fait que vous ne pouvez pas authentifier qui possède quel bloc d'adresses IP. Qui parmi vous travaille avec les routeurs ? Je suis très jaloux. Ils ont pris tous mes mots de passe habilités il y a quelques années. Je ne suis plus autorisé à travailler avec les routeurs.

Vous pouvez le procurer entre deux puristes, deux personnes qui parlent. Vous pouvez utiliser MD5 ou un autre algorithme pour authentifier qui vous êtes. Vous ne pouvez pas le faire à l'échelle mondiale. Il y a eu plusieurs tentatives pour corriger cela. Assurer le BGP en est une. Le BGP est le protocole de routage, une version sécurisée et ce qu'on appelle RPKI, infrastructure de gestion de clés. Aucun des deux n'a vraiment été déployé jusqu'à maintenant. Donc voilà le genre de questions de sécurité que nous examinons.

Il y a autre chose que l'on appelle marché gris, le marché émergent, le marché de l'IP Version 4.

Peut-être vous pensez que ce n'est pas un problème de sécurité. Pourquoi le fait que les gens achètent et vendent des adresses IP est un problème de sécurité ? Ce n'est pas un problème de sécurité, mais il pourrait être un problème de stabilité. Que se passerait-il si d'ici cinq ans ou deux ans, les adresses

deviendront si chères et si limités qu'aucun de vous ne pourra les obtenir ? En quelque sorte cela signifie que vous ne pouvez pas même faire la traduction que nous faisons entre v4 et v6. Je ne veux pas dire que ça va arriver, mais c'est quelque chose à laquelle nous devons penser, et on a déjà commencé à étudier cette question.

Je dirais qu'il y a environ cinq ou six ans, nous avons eu un atelier organisé par Google qui analysait si oui ou non il y aurait un marché émergent. Nous avons prédit que ce marché existerait, et nous avons analysé si nous pourrions établir des contrôles. On a travaillé avec les meilleurs économistes et les meilleurs ingénieurs du monde et nous n'avons pas pu résoudre la question. Alors, voilà le genre de choses que nous analysons dans l'espace d'adresses.

De toute évidence, l'épuisement des ressources d'IPv4 est quelque chose que nous avons étudiée pendant des années et nous avons essayé que les gens comprennent que cela allait devenir une réalité. Malheureusement, les gens ne vous croient jamais vous quand vous leur dites que le ciel va tomber jusqu'à ce qu'il leur tombe sur la tête.

Nous l'avons dit, « IPv4 s'épuise. IPv4 va s'épuiser. Non, sérieusement, ça va s'épuiser très bientôt, bientôt ».

Tout le monde le dit, « oui, oui, ... » et puis un jour, IANA, le bloc de l'ICANN, vient à manquer.

Nous essayons de prévoir ce genre de choses, même si les gens n'écoutent pas. Nous nous penchons sur ce genre de choses plutôt que d'entrer dans le détail en matière de sécurité.

FEMME NON IDENTIFIÉE : [inaudible]

JOHN CRAIN : Ouais.

FEMME NON IDENTIFIÉE : Tout d'abord, je pense que les RIR se penchent aussi sur les questions de RPKI et IPv6.

JOHN CRAIN : Absolument.

FEMME NON IDENTIFIÉE : Alors, où est la frontière entre ce que l'ICANN fait et ce que font les RIR ? Deuxièmement, au début, je pensais que votre groupe travaillait au niveau de l'infrastructure, mais maintenant il semble que vous travaillez sur des opérations de bout en bout. C'est correct ?

JOHN CRAIN : Nous nous occupons aussi bien des protocoles. Nous nous occupons de ce que les identificateurs utilisent. La question centrale c'est le système d'identificateurs. Ce sont les noms et les adresses, les numéros de port, tous les systèmes d'identificateurs. Et oui, les RIR s'occupent, bien sûr, de tout ce concernant les adresses IP et aussi, bien sûr, des numéros du système autonome. Alors, nous travaillons ensemble.

J'ai l'habitude de travailler à la RIPE NCC. Ils ont ce que l'on appelle les laboratoires RIPE, à savoir un centre de recherche dans un des RIR, et nous travaillons très étroitement avec eux. En fait, qui a entendu parler du programme ATLAS ? Nous sommes un des sponsors de ce programme. Daniel Karrenberg, le gars qui l'a conçu, est l'un de mes meilleurs amis, donc nous travaillons sur ce genre de trucs ensemble.

Alors, y a-t-il une frontière ? Certainement, quand vous arrivez dans la sphère politique, mais quand on a affaire à des problèmes réels, nous avons tendance à travailler beaucoup ensemble.

OSAMA TAMIMI : Bonsoir. Je suis un boursier de l'ICANN du Pakistan. J'ai juste une préoccupation générale. Vous vous occupez de la sécurité

du point de vue de l'ICANN ? Vous vous concentrez uniquement sur DNSSEC ou vous visez à quelque chose de plus vaste pour avoir une sécurité de l'Internet de bout en bout ?

JOHN CRAIN : Non, nous nous concentrons sur la sécurité de l'identificateur, non seulement du DNS. Nous ne visons pas à la sécurité de bout en bout. Ce n'est pas nous qui faisons ça. Nous ne construisons pas des produits de sécurité. Nous ne sommes pas ciblés profondément dans l'infrastructure d'autrui. On ne peut pas. Ce n'est pas notre rôle. Notre rôle, tel que prescrit dans nos statuts, dès que notre groupe a été formé, est de nous centrer sur la sécurité et la stabilité. Nous avons ajouté la résilience parce que vous en avez besoin lorsque les choses vraiment se cassent, du système d'identificateurs dont le DNS en est un. Il est important, mais ce n'est qu'un.

HAMZA MEHREZ : Hamza Mehrez de la Tunisie. J'ai une question qui peut être liée à la sécurité en ligne des utilisateurs finaux. Ma première question : pensez-vous que les utilisateurs finaux devraient utiliser l'Internet anonymement ? Et la deuxième question est la suivante : quelles sont vos recommandations pour les menaces au développement de l'Internet des objets ?

JOHN CRAIN : Bon, alors voilà deux questions distinctes. Les gens devraient pouvoir jouir de la confidentialité. Et l'anonymat, mot que je trouve horrible – anémone, le personnage de la bande dessinée avec le poisson – c'est une question différente. D'une part je dis, « oui, vous devriez pouvoir être anonyme ». Mais si d'autre part je dis : « Eh bien, si vous m'attaquez vous êtes un criminel, ou quoi que ce soit, je ne veux pas vous permettre d'être anonyme ». Je veux l'application de la loi à travers une procédure officielle pour avoir un moyen de vous identifier. N'oubliez pas la partie de la procédure officielle qui est très importante.

J'ai moi-même un conflit à cet égard parce que bien des fois je voudrais être absolument anonyme. Quand je regarde Facebook au travail, je ne veux pas que mon patron sache que c'est moi qui me promène sur Facebook toute la journée, mais je comprends aussi l'autre côté de l'argument. Alors, ce n'est pas une question facile à résoudre. Si c'était une question facile, il ne faudrait pas tellement lutter à cet égard.

Quelle était, déjà, la seconde question ?

STEVE CONTE : L'Internet des objets.

JOHN CRAIN : Oh, l'Internet des objets. J'ai un souci au sujet de l'Internet des objets, et c'est qu'ils sont tous très bon marché. Les dispositifs sont bon marché. Ils ne sont pas aussi sûrs qu'ils devraient l'être. L'Internet des objets est un terme de marketing pour mettre tous vos appareils sur Internet, tout comme la cybersécurité est un terme de marketing. Il y a beaucoup termes de marketing ayant trait au nuage. Ce sont tous des termes de marketing.

Pourquoi suis-je inquiet ? Je joue avec des appareils à la maison tout le temps. Mes interrupteurs d'éclairage... je peux contrôler mon téléphone. J'ai des caméras. On ne peut pas faire tout cela en dehors de la maison. Je ne peux pas le faire d'ici parce que la question de la sécurité m'inquiète, mais dans un réseau contrôlé, je joue avec ces choses tout le temps.

Franchement, la plupart ne sont pas très bien construits, mais c'est la nouvelle technologie. Les voitures n'étaient pas très bien construites au tout début, alors, ce genre de choses, elles sont petites, elles sont moins chères. Ça va aller mieux, je l'espère.

STEVE CONTE : [Inaudible] à cela aussi, si je le pouvais. C'est OK. J'ai un micro. La première question que vous aviez. Oui, nous travaillons à l'ICANN, et nous avons une cible très limitée et précise sur ce que l'on fait en matière de sécurité, de stabilité et de résilience.

L'utilisateur ou la connectivité de bout en bout ne sont vraiment pas des questions du ressort de l'ICANN, mais soyons honnêtes. Nous sommes tous des utilisateurs finaux, alors nous avons tous nos propres préoccupations personnelles et nous essayons de trouver un équilibre entre les préoccupations personnelles, lu travail, et des choses du genre.

Il y a certains chevauchements là-dessus, mais John l'a mentionné. Cela n'est pas de la compétence de l'ICANN. Si l'ICANN agissait au delà de ses attributions, alors nous serions dans un territoire que d'autres experts analyseraient. Collaborer avec eux est une chose, mais marcher sur les platebandes d'autrui c'est autre chose. Alors, nous essayons de collaborer avec ces groupes, lorsqu'il est pertinent de le faire.

Pour l'Internet des objets, je pense que ce que nous voyons, c'est une période de développement rapide du produit. Avec un développement rapide, cela dépend plutôt de la part de marché plutôt que de la sécurité et la connectivité, et la sécurité, et tout ça. Tout le monde est si dans le vent et enthousiasmé par l'Internet des objets... Ils ignorent le processus d'élaboration du protocole approprié, des fois vieilli, des fois lent, à travers l'IETF, qui garantit la sécurité pour l'élaboration du protocole. Les gens veulent juste que ça fonctionne.

Parfois, c'est génial. Il y a quelques bons services et des bonnes choses quant à l'Internet des objets, mais il faut respecter le processus et comprendre que si on ne le fait pas, il va y avoir des conséquences. Le nombre croissant de questions liées à l'Internet des objets, eh bien, ça va commencer à faire un mélange...

Nous commençons à voir le problème depuis différents aspects. Rick travaille sur des trucs du DNS et de l'IoT. Nous avons commencé à analyser la question et à nous immerger un peu pour voir s'il y a quelque chose qui relève de la compétence de l'ICANN, mais en ce moment, nous voyons seulement la question en tant qu'individus.

JOHN CRAIN : Oui, et si vous regardez tous ces périphériques, beaucoup d'entre eux ont des serveurs DNS. Ils vont tous avoir besoin des adresses IP. Ils vont tous être une sorte d'adresse IP privée ? Ce sera IPV6 ? Il y a beaucoup de questions qui nous concernent, mais ce n'est pas parce que c'est l'Internet des objets. C'est parce que tout cela affecte notre monde.

Quelqu'un d'autre ? Lequel ? Vous êtes le modérateur. D'accord, qui était en premier lieu ? Commençons par ce monsieur. Son micro marche ? Allez-y. Non, ce monsieur.

HOMME NON IDENTIFIÉ : [inaudible]

JOHN CRAIN : Oui, tout à la fin.

HOMME NON IDENTIFIÉ : D'accord, merci. Merci beaucoup. J'ai cette clarification sur deux [inaudible] de votre part. Comment ça se passe avec le contrôle de la sécurité quand vous le comparez avec le contrôle du gouvernement ? Car où la [inaudible]. Je suis très intéressé à cette question aussi. Mais que se passe-t-il quand les gouvernements choisissent de contrôler notre sécurité sur le domaine. Je ne sais pas à quel moment ils font ça.

Je vais donner un exemple. À un certain moment, mon pays et les [inaudible] est mon nom du Nigeria, soit dit en passant. À un certain moment, je ne me souviens pas ce qui se passait à ce moment-là, mais la période [inaudible] [inaudible] ou 24 environ, il n'y avait pas d'Internet. Vous ne pouviez absolument vous connecter à aucun domaine. Les téléphones ont été bloqués. Je ne parle pas du téléphone de toute façon, mais l'Internet, vous ne pouvez pas vous connecter. Nous ne pouvons pas vous connecter au site de l'ICANN. On ne peut pas ouvrir une session.

À quel moment voit-on les sécurités ? Par ailleurs, il y a un [inaudible]. Le [inaudible], c'est que la même personne qui est intéressée à bloquer le site Web peut être intéressée à compromettre la sécurité.

JOHN CRAIN : Les gouvernements font ce que font les gouvernements. Vous parlez de l'Internet et pas du système d'identificateurs. Il y a eu des cas où les gouvernements ont décidé de couper la bande passante pour couper l'accès. Si nous regardons, nous disons: « Y a-t-il un effet sur notre écosystème ? »

Juste parce que quelque chose ne fonctionne pas dans le pays, cela ne veut pas dire que cela ne fonctionne pas dans le reste du monde. Pendant longtemps le DNS et tout pour tout le monde en dehors de ce pays, tout à fait bien, au moins si leurs systèmes ont été construits correctement.

Les gouvernements font ce que font les gouvernements. Cela n'a rien à faire avec nous. Ce sont des questions concernant les politiques nationales.

Il y a eu des cas où des choses comme ça sont arrivées, et les gens disent : « l'ICANN a éteint ce pays, » parce que les médias disent ce qu'ils veulent. Rien de tel n'est jamais arrivé. Nous n'avons jamais eu la pression des gouvernements pour

participer à ce genre de choses. Bien que je soupçonne que si nous l'avions fait, ils diraient « ouais, ne vous y mêlez pas ». Les gouvernements font ce que font les gouvernements. Ce n'est pas vraiment notre domaine.

Ce qui est intéressant c'est qu'il y a un grand nombre de gouvernements qui participent aux processus de l'ICANN, et quand ils sont ici, ils aiment tous l'Internet. Bon, la plupart. Ils disent, « C'est très important », et puis parfois, vous voyez – et c'est très rarement – vous voyez que l'accès à l'Internet est coupé, et cela n'est pas toujours fait exprès, soit dit en passant. J'ai pu voir que cela est arrivé, mais ça n'a été qu'un accident.

C'est un sujet intéressant, mais l'ICANN ne s'y mêle pas vraiment. Le GAC ne se mêle jamais de ce genre de choses. Ce n'est pas notre domaine.

[BOB] : Merci. Je voulais vous demander sur la confiance du public, sur l'infrastructure publique. Quel avenir voyez-vous entre l'avenir des autorités de certification et l'utilisation de l'authentification basée sur les DNS d'entités nommées ?

JOHN CRAIN : Vous dites quant est-ce que DNSSEC intervient. C'est comme n'importe quoi. Vous avez besoin d'applications que les gens

vont utiliser. Personnellement, j'aimerais qu'à un certain moment DNSSEC soit omniprésent et que les gens ne pensent vraiment plus à cette question. Cela voudrait dire que le DNS est sûr. Cela pourrait prendre des années.

Ce qui est intéressant c'est que DANE arrive. Il s'agit d'une partie de l'IETF qui offre des services au-dessus du DNSSEC si vous voulez, la capacité d'avoir vos propres certificats et par la suite les authentifier, en quelque sorte. Si les gens commencent à utiliser des choses comme ça, si on fait des expériences, le fait d'avoir DNSSEC peut avoir plus d'avantages que d'avoir seulement l'authentification de vos réponses. Ce sera intéressant, et ça ne fait que commencer.

La personne que vous pouvez contacter et que je peux vous présenter, est un monsieur qui s'appelle Dan York de l'ISOC qui s'occupe de mesurer ce genre de choses. Monsieur Richard Lamb mesure aussi ce genre de choses, mais l'ISOC a beaucoup de détails sur comment cela se développe et le public commence à utiliser DANE et autres choses au-dessus du DNSSEC.

Si nous ne construisons rien de plus sur le DNSSEC, si nous n'utilisons pas l'outil, alors, il faudra se débrouiller. C'est la même chose pour l'IP version 6. Si on n'a pas une raison pour l'utiliser, eh bien, on ne l'utilise pas. Les gens utilisent ce qu'ils

connaissent. La raison en est que le ciel est tombé et IPv4 est épuisé, mais tout ce que l'IPv6 a promis n'a vraiment jamais intéressé personne.

Je pense que vous étiez le prochain.

MUHAMMAD SHABBIR : Merci. Je voudrais savoir si vous pouvez nous parler un peu des techniques et des outils que vous utilisez pour assurer la sécurité de l'identificateur. Quelles sont les techniques, si vous pouvez nous éclairer à ce sujet ? Et pour mémoire, c'est Muhammad Shabbir du Pakistan.

JOHN CRAIN : Les outils sont très simples. Évidemment, il y a la recherche, pour mesurer ce qui se passe, pour identifier les différences. Mais il y a aussi quelque chose que l'on appelle intelligence vis-à-vis de la menace ; on parle aux gens, on organise des listes de diffusion sur la sécurité, on est partout où on parle de ces questions. Ce sont des concepts de base. Il n'y a rien de majeur.

Nous avons certains laboratoires. Par exemple, nous avons un laboratoire où nous regardons comment les paquets changent pendant qu'ils vont à travers les logiciels médiateurs, des choses comme les routeurs, les pare-feux et les VPN. Toutes ces choses ont des conséquences sur les paquets et les identificateurs.

Nous menons des recherches. Nous avons un petit groupe de recherches.

Puis, autre chose que nous faisons, nous interagissons avec la communauté. Nous parlons constamment aux gens de la communauté de la sécurité de ce que l'on voit. S'il y a une menace, ils savent qu'ils doivent nous appeler. Si nous examinons certains parmi les grands réseaux zombies qui ont causé des problèmes sur le réseau mais qui ont aussi affecté le système d'identificateurs, on peut voir qu'ils constituent une menace à la fois parce qu'ils peuvent être utilisés pour faire un DDoS au système, mais aussi, souvent, parce qu'ils enregistrent des dizaines de milliers de noms dans le système qui ne sont là qu'à des fins néfastes, et nous pensons que cela est un problème.

La plupart, nous ne les trouvons pas. Ce n'est pas notre domaine d'expertise, mais nous connaissons les personnes qui s'occupent de la question et ils nous connaissent. Le fait d'identifier les menaces et voir comment elles approchent ne veut pas dire que vous connaissez tout. Il s'agit d'avoir des groupes de pairs pour pouvoir apprendre des autres.

Je vous ai vu. Je viendrai à vous ensuite. OK, allez-y.

HASHIM NOUMAN : Hashim Nouman du Pakistan. Que faites-vous pour arrêter les CGN ?

JOHN CRAIN : Rien. Des NAT à grande échelle. Rien. Nous observons avec perplexité.

STEVE CONTE : Et aussi un peu d'instabilité à ce sujet.

JOHN CRAIN : Ouais, et un peu d'instabilité. Si vous utilisez un NAT à grande échelle ou vous allez avec quelque chose comme v6, que je préfèrerais, il s'agit là d'une décision commerciale. Les gens regardent cela d'une perspective commerciale.

Maintenant si vous êtes du côté qui veut voir ce qui se passe pour la détection de la vulnérabilité, la recherche de mauvais acteurs, des choses comme ça, cette grande échelle [NAT-ing] d'adresses et les problèmes liés à cet enregistrement sont problématiques.

Mon inquiétude personnelle sur les NAT à grande échelle est que les gens investiront beaucoup d'argent pour les utiliser - ce n'est pas bon marché - et puis ils n'auront, possiblement pendant longtemps, aucune motivation pour passer à v6. Si cela vient par

défaut, tous les grands FSI disent : « Eh bien, les NAT à grande échelle, parce qu'ils ont toutes ces fonctions étonnantes, c'est ce que nous allons faire » pour tout propos commercial qu'ils puissent avoir. Je m'inquiète pour l'effet sur le déploiement et l'adoption de v6 en dehors des bouts, etc. Mais ce sont des décisions commerciales, très difficiles à influencer.

STEVE CONTE : Juste un commentaire. Je suis tout à fait d'accord avec ce que John vient de dire. Mais lorsque vous utilisez le CGN et des choses comme ça et même plainnat, vous ou votre appareil changent ce que le paquet était censé être en premier lieu. Si vous modifiez déjà votre véritable connectivité de bout en bout juste en mettant un NAT unique quelque part.

Je reconnais que cela est valide. J'ai un tout un réseau. J'ai un NAT et je l'utilise, mais quand vous mettez NAT sur NAT sur NAT sur NAT, puis vous cassez beaucoup plus et beaucoup plus et beaucoup plus encore. Ce n'est pas un problème de l'ICANN, mais c'est une question à laquelle il faut faire attention. Je suis certain que d'autres personnes veulent savoir si oui ou non cela casse des choses et à quel niveau.

Comme Jean l'a dit, c'est une décision commerciale. Si un FSI décide d'utiliser CGN et ça casse leur base de clients, c'est horrible pour le client. Je suis d'accord, mais cela n'affecte pas

nécessairement la stabilité ou la résilience de l'Internet dans son ensemble. Sauf pour quelques hallucinations massives bizarres, étranges, nous décidons de mettre CGN vraiment au cœur du routage, et puis, quand les choses ne marchent pas, cela devient vraiment le problème du client ou de l'entreprise. Ce n'est pas une grande réponse, mais voilà où nous en sommes.

JOHN CRAIN : Il faut aussi se rappeler que chaque fois que nous intervenons dans des domaines qui sont gris pour nous, on nous tire dessus. Nous recevons des pressions pour rester dans vos limites. Alors, des choses de ce genre, elles sont vraiment dans cette zone grise. Nous sommes impliqués dans des discussions, parce que les gens viennent à nous à cause de notre expertise, et nous voulons apprendre. Mais cela ne veut pas dire que l'ICANN élaborerait une politique là-dessus, ou des choses du genre. Ce n'est pas dans sa sphère d'action.

Avez-vous un commentaire à ce sujet ou une question ?

HOMME NON IDENTIFIÉ : [inaudible] CGN ?

JOHN CRAIN : Vous voulez faire quoi ?

HOMME NON IDENTIFIÉ : Savez-vous ce que c'est que le NAT ? Si vous avez un routeur, vous avez une adresse IP publique, le routeur transforme cela dans de multiples adresses IP ? Un NAT à grande échelle est la même chose mais, curieusement, à grande échelle. Si une compagnie de téléphonie cellulaire ou un câble ou un FSI, en raison de la diminution et de l'épuisement d'IPv4, a beaucoup d'IP publics mais sa base clients est 1000 fois le nombre d'adresses IP publiques disponibles. Ils transforment cela en un grand NAT au début de leur réseau.

JOHN CRAIN : Par exemple, vous conservez les adresses pour des intervalles de temps très courts. Les durées du bail sont vraiment courtes, l'enregistrement qui doit changer est vraiment dur, ils disent.

HOMME NON IDENTIFIÉ : En termes de taille intensive, aussi.

JOHN CRAIN : Ce Monsieur au fond de la salle.

HOMME NON IDENTIFIÉ : C'est le même.

JOHN CRAIN : Oh, vous avez changé de place. Ne bougez pas.

[JOHN CHAND] : Salut, John de Fidji. En parlant de la sécurité du DNS, quelles sont les menaces d'imagerie pour le DNS ? Première question. Et la deuxième question est : comment traitez-vous la déontologie des négociants [éthique dealers'] sur les serveurs DNS ?

JOHN CRAIN : Votre deuxième question a répondu la première. L'un des plus gros problèmes, à mon avis, est le DDoS. Nous avions beaucoup de problèmes avec des questions comme l'empoisonnement du cache. Il y en a moins maintenant, grâce à différentes solutions. Vous voyez ces problèmes, vous cherchez des solutions. Les buy-ins et tous les autres serveurs ont fait des ports aléatoires pour que ce soit plus difficile de savoir quel port serait utilisé.

Je suis désolé si mon approche devient trop technique. C'est difficile de ne pas le faire lorsque l'on aborde ce type de questions.

Au début il y a le DNSSEC et l'empoisonnement du cache, le mensonge sur les noms du DNS sont plus profonds. Il y a des

moyens de le faire. Ces moyens ne sont pas parfaits. Au fur et à mesure du déploiement du DNSSEC, etc. ça devient de mieux en mieux.

Qui a fait l'objet d'un DDoS ? Attaque par déni de service, qui fait tomber votre réseau. C'est une situation vraiment lamentable. Il n'y a pas grand-chose à faire à ce sujet. Vous approvisionnez de plus en plus, ce qui est cher, et vous avez votre provision du FSI en amont, et vous pouvez faire un peu de filtrage.

Mais si quelqu'un veut vraiment vous faire un DDoS, vous aurez des problèmes. Vous avez vu vraiment de grandes organisations qui ont fait l'objet de DDoS, des sociétés qui ont des fonds de milliards de dollars pour acheter de l'infrastructure et qui font toujours l'objet de DDoS.

Auparavant, on voyait une tendance importante de la croissance des DDoS individuels, et ça continue... Je n'ai pas examiné les dernières statistiques, mais nous avons vu des DDoS dans la gamme des demi-téraoctets.

Qui a ici une bande passante de demi-téraoctets dans son réseau ? Oui, personne. Mais ce que nous voyons maintenant, ce sont des DDoS de plus en plus petits. Nous voyons qu'on les utilise pour différents types d'activités criminelles. Bien des fois les grands disaient comme expression politique : « je ne vous aime pas, alors je vais vous faire disparaître »... Mais maintenant,

nous voyons beaucoup de chantage et de choses du genre. Nous voyons beaucoup d'extorsion à travers le crime.

En raison du DDoS, des réseaux zombies, des réseaux de machines compromises, à mon avis, voilà un des gros problèmes du réseau et nous n'avons pas trouvé une bonne solution. Même quand on sait où ils sont (nous avons des moyens pour le faire) nous faisons attention aux réseaux zombies parce que nous pensons qu'ils sont une menace – même si nous identifions une machine qui est compromise et qu'elle fait partie d'un réseau zombie, nous n'avons vraiment pas grand-chose à faire à ce sujet. C'est des victimes, mais nous ne pouvons même pas résoudre le problème de leur machine car ce serait illégal.

Les criminels peuvent s'en tirer avec ce genre de choses parce qu'ils s'en fichent, mais vous, dans la plupart des juridictions, vous ne pouvez pas vraiment aller et réparer la machine de quelqu'un d'autre sans son consentement explicite.

Ainsi, lorsque nous voyons comment ça se passait il y a quelques années... il y avait des adresses IP et des millions de machines infectées, mais nous pouvions entrer en contact avec les FSI et avec un peu de chance ils pouvaient faire quelque chose. En fait, nous ne pourrions rien faire même du point de vue technique, mais probablement nous pourrions le faire parce que

nous avons ici dans la salle des gens très intelligents. Vous pouvez dire « Si on faisait cela, nous pourrions nous en sortir ».

STEVE CONTE : Mais n'oubliez pas que le propriétaire de la machine compromise n'est pas le méchant. C'est votre maman.

JOHN CRAIN : Du point de vue moral et juridique, ce n'est pas la bonne chose à faire. Je crois que, de loin, c'est probablement la plus grande menace. Nous avons en fait un document qui répertorie un grand nombre de différentes menaces à l'écosystème, mais un grand nombre des menaces, si vous regardez la réalité, concernent le côté commercial et pas le côté technique. Mais le DDoS, est de loin la plus grande menace en ce moment.

HOMME NON IDENTIFIÉ : [inaudible]

JOHN CRAIN : Inaudible. C'est lui.

HOMME NON IDENTIFIÉ : Je m'appelle [inaudible] de la Gambie, je suis boursier pour la deuxième fois. Ma question, je voudrais revenir à l'Internet des

objets. Ma question est, l'Internet des objets est vraiment nécessaire ? Pourquoi en avons-nous besoin ? Parce qu'à mon avis, il n'y aucun [inaudible] pour inventer l'Internet des objets.

STEVE CONTE : Vous avez un téléphone portable ?

HOMME NON IDENTIFIÉ : Ouais. OK. Encore une fois, ma deuxième question est quelles sont les politiques ? Quelles sont les règles ou les lois en vigueur qui nous permettent de protéger les personnes avec tous les défis de sécurité auxquels nous sommes confrontés ? Parce que de nos jours vous n'avez même pas besoin de compétences techniques pour être un pirate informatique parce que tous les outils sont disponibles en ligne où vous pouvez les télécharger gratuitement. Alors, n'importe qui peut pirater. Quelles sont donc les politiques ou les règles en vigueur pour protéger ces programmes ou ces logiciels de l'accès facile ?

JOHN CRAIN : C'est un marché ouvert. Il n'y a aucune règle réelle. Il y a des lois. Il existe des lois dans tous les pays. Si vous faites un DDoS à quelqu'un pour lui extorquer de l'argent, ça c'est l'extorsion. C'est un crime dans ce pays. Le problème est que la plupart de tout ça n'est pas dans un pays. La victime peut être dans un

pays, mais tout passe à travers les juridictions. Il y a des conventions comme la Convention de Budapest et d'autres pour les organismes d'application de la loi. Ces questions ne sont pas du ressort de l'ICANN. Nous ne sommes pas application de la loi. Nous ne sommes pas un gouvernement. L'application de la loi et la protection de la société sont vraiment du ressort du gouvernement, et c'est eux qui font les lois.

Maintenant, beaucoup d'anciennes lois, c'est-à-dire les lois physiques, vous pouvez réellement les utiliser pour l'Internet. Le crime est toujours le crime. Il y a très peu de crimes qui soient vraiment des crimes d'ordinateur à ordinateur. Il y a très peu de crimes qui soient vraiment des cyber crimes. Normalement, ce sont des crimes contre les personnes ou contre les biens, et il y a plein de lois qui s'en occupent.

Maintenant, il est vraiment difficile d'apprendre aux juges, aux avocats et aux législateurs à penser comme ça et qu'ils comprennent ces choses. L'Internet est assez nouveau. Nous avons un long chemin à parcourir, mais ce n'est pas le travail de l'ICANN. C'est un travail des gouvernements et des gens qui conseillent les gouvernements.

Avons-nous besoin de l'Internet des objets ? Eh bien, Steve vous a demandé si vous aviez un téléphone. C'est un objet. C'est sur

Internet, si vous avez besoin de cette petite partie de l'Internet des objets.

STEVE CONTE : Oui, je vous ai demandé de penser à l'Internet des objets. Je pense que cela peut aider. Il fallait trouver une manière d'établir qu'il y a désormais plus de dispositifs que de gens sur Internet. Avant, il y avait un ordinateur par famille et tous ses membres, quatre ou cinq, partageaient cet ordinateur. Alors à ce moment-là, il y avait plus de gens que de dispositifs. Maintenant ce n'est plus le cas. Je pense que si vous pensez à l'Internet des objets comme une manière différente de penser ce qui est sur Internet et laisser de côté l'aspect de marketing, eh bien, c'est vraiment ce que c'est. C'est juste un déploiement rapide de plusieurs dispositifs qui se trouvent sur l'Internet.

JOHN CRAIN : Oui, et vous pouvez poser la question si vous voulez ou pas que votre ampoule électrique soit contrôlée par votre téléphone. En avez-vous besoin ? Avoir besoin est un grand mot. Vous avez besoin de nourriture. Vous avez besoin d'eau. Vous avez peut-être besoin d'une forme quelconque de pouvoir, bien que vous puissiez probablement vivre sans ce pouvoir. Alors, avoir besoin est un grand mot. Il y a clairement un marché. Il y a clairement de bons usages de l'Internet des objets.

Alors, si je joue à la maison parce que j'aime jouer avec ces choses-là et il y a un incendie, mon alarme contre incendie va se déclencher. Nous avons tous ça, mais mon alarme est effectivement connectée au réseau. Alors, lorsqu'elle se déclenche, que se passe-t-il ? Toutes les lampes de la maison deviennent orange et cela parce que la couleur orange se voit dans la fumée. Si la fumée est détectée, elle peut être envoyée à l'extérieur à travers le système de climatisation.

Parfois, les objets peuvent être plus intelligents et plus utiles et ils ont effectivement des propriétés de sauvetage lorsque la communication est bonne. Tout va mal quand la sécurité échoue, mais il y a des dispositifs utiles et clairs et lorsque vous les connectez, ils gagnent tout à coup une toute nouvelle vie.

Pensez à un thermostat que vous pouvez avoir chez vous. Combien parmi vous changent la température du thermostat à chaque fois que vous pensez qu'il faut un ajustement ? Vous allez, « Oh oui, je vais juste le laisser. Il diminuera ». Ou vous pouvez le faire une ou deux fois par semaine ou une fois par jour, selon la température. Le thermostat marchera à maintes reprises alors que cela n'est pas nécessaire. Cela signifie gaspiller de l'énergie. Si vous regardez certains de ces thermostats d'apprentissage qui ont des algorithmes et qui peuvent être programmés à distance, par exemple, mon thermostat. Je peux conclure un contrat avec ma compagnie

d'électricité (ce que je n'ai pas fait parce que je ne leur fait pas confiance) pour accéder à un programme qui, lorsque la température monte au-dessus d'un paramètre déterminé, mon système reviendra à la température appropriée. Pour ne pas trop refroidir. C'est un usage réel. Si vous avez une ville entière de gens qui font ça, vous faites vraiment la différence dans l'écosystème.

Avoir besoin est un grand mot. Je ne pense pas que nous ayons besoin d'aucune de ces choses. Nous n'avons pas besoin de l'Internet. Besoin. Mais mon vieux, cela rend la vie plus facile. Vous n'avez pas besoin des téléphones mobiles, mais ils sont très pratiques. Vous n'avez pas besoin des thermostats qui se connectent à l'Internet. Je n'ai pas réussi à comprendre quel est le motif pour qu'un réfrigérateur soit connecté à l'Internet, mais les gens me disent qu'il y en a. Ou un grille-pain. Mais c'est le marché qui va décider.

Je pense que beaucoup de gadgets vont disparaître au fil du temps, tandis que d'autres seront extrêmement utiles.

STEVE CONTE : John, le patron a dit deux questions, mais vous êtes bavard, alors, une question de plus pour que tout le monde puisse sortir à l'heure.

JOHN CRAIN : Je ne suis pas bavard. J'aime beaucoup parler, tout simplement. On va prendre deux questions et les réponses seront courtes. Tout d'abord le monsieur qui est là et puis l'autre qui n'ont pas encore posé de questions.

ANAND RAJE : Anand Raje, boursier de l'Inde. Nous assistons à une très grande transformation dans le cyberespace pour aller vers l'Internet des objets au fur et à mesure que l'IPv6 [inaudible] commence. Je vous demande votre commentaire d'expert. Pensez-vous que dans dix ans nous serons sur Internet, parce nous voyons maintenant que les systèmes comme les serveurs racine ouverts européens [inaudible] le DNS est à venir. Ensuite, il y a des systèmes anonymes jonglant comme web profond et web obscur. Et les questions liées à la confidentialité sont là. Il y a des voitures sans chauffeur, donc les objets sont là.

Alors, qu'en pensez-vous ? Où en serons-nous dans dix ans ?

JOHN CRAIN : Eh bien, je ne peux pas prédire l'avenir, mais je peux faire deux petits commentaires rapides pour répondre à ce monsieur. Ces autres systèmes DNS alternatifs, s'ils peuvent trouver un moyen d'être communiqués, ce serait génial. Je ne pense pas qu'ils

vont le faire parce que nous avons dit cela depuis années. S'ils vont tous par des chemins séparés, ce ne sera pas l'Internet. Il y aura des Internet, et puis peut-être, nous ne serons pas en mesure de nous communiquer entre nous. Il faut donc trouver un moyen, si nous allons de l'Internet vers les Internets, pour traverser les frontières. Parce que je ne dis pas que ce soit bien ou mal. Personnellement, j'ai des problèmes avec cette question. J'aime l'idée que si j'envoie un courrier électronique, il arrive toujours au même endroit. Il y a peut-être une technologie permettant de résoudre la question. Il y a des gens qui travaillent là-dessus.

Nous ne savons pas ce que l'Internet sera dans dix ans. Il y a de nouvelles technologies qui vont et qui viennent. Peut-être que le DNS n'existera même plus. Qui utilise vraiment ici le DNS dans sa vie quotidienne ? Steve et moi, et nous sommes bien bizarres. Normalement, on utilise les moteurs de recherche et les applications. Peut-être que cela est dans l'arrière-plan mais sans importance pour l'utilisateur actuel. À un certain point, les gens seront moins avides et politiques à ce sujet parce sa valeur ne sera pas aussi grande. Cela peut changer, mais seulement à travers la technologie.

Je vais laisser la parole à ce monsieur.

HOMME NON IDENTIFIÉ : [inaudible]

JOHN CRAIN : J'invite Steve à répondre à cette question, quelle qu'elle soit...

[HAMAD USAMA] : [Hamad Usama] du Maroc. Bienvenus au Maroc. Ma question porte sur votre future stratégie dans votre nouvelle stabilité et résilience et comment nous pourrons les mettre en œuvre à l'avenir. En ce qui concerne la deuxième information sur l'Internet des objets, nous avons organisé la confiance de l'Internet des objets en termes de [inaudible]. C'est très intéressant, mais normalement les gens ignorent pourquoi cela est nécessaire. C'est pour [faciliter] notre vie ou tout simplement pour être en ligne avec la nouvelle technologie. Merci.

JOHN CRAIN : Je vous l'ai dit, vous avez donné la réponse.

STEVE CONTE : Alors, pour répondre à la première question, demandez à John. Pour en revenir à l'Internet des objets, je ne pense pas que ce soit déjà plus une question de nécessité ou de volonté. Si nous regardons le système téléphonique au cours des 100 dernières années, 120 même, c'est un peu comme le modèle d'Internet

seulement si vous l'aviez. De plus en plus de gens ont utilisé le système téléphonique, et tout à coup, tout le monde pouvait l'utiliser, et maintenant votre téléphone est dans votre poche. Si votre téléphone voyage dans votre poche, eh bien, c'est la partie de l'Internet des objets. Maintenant nous avons l'Internet et cela depuis 25 ans. L'Internet a été utilisé de plus en plus et alors les entreprises ont décidé de vendre des choses sur Internet. Maintenant, nous sommes au point où tout parle sur Internet. Il n'est pas nécessairement question que nous ayons besoin ou que nous voulions avoir des choses. C'est un peu ce que John a dit. Son système parle à d'autres dispositifs qui, par conséquent, améliorent sa vie ou la rend plus sûre ou des choses du genre.

On pourra voir ce qu'il y a dans le réfrigérateur à travers la télé qui organisera les achats automatiquement, et ça, ce n'est pas l'Internet des objets. L'Internet des objets sont ces petits capteurs, minuscules, qui travaillent de concert pour que la vie des utilisateurs devienne de plus en plus pratique. Je pense que c'est ce qui va se passer. Il n'est pas nécessaire d'avoir un surnom, une étiquette de l'Internet des objets. L'humanité travaille dur pour ne pas travailler. C’est donc ça que nous faisons. Nous travaillons dur afin que nous ne soyons pas obligés à travailler.

JOHN CRAIN : Première question, stratégie. Lorsque nous avons parlé de la stratégie SSR... nous sommes sur le point de publier un nouveau document.

STEVE CONTE : Stratégie SSR ? Le cadre ?

JOHN CRAIN : Oui, le cadre.

STEVE CONTE : Notre cadre, nous avons un nouveau cadre pour la SSR. Il sera publié sur notre site, probablement le mois prochain.

JOHN CRAIN : Nous devons publier nos prévisions stratégiques pour les prochaines années, et nous le faisons quasiment tous les ans. Nous analysons ce que nous croyons peuvent être des possibles menaces émergentes, alors, il faut planifier à l'avance.

STEVE CONTE : Et puis nous demandons à la communauté d'en faire la révision. C'est un double processus. On dit, « C'est ce que nous pensons que nous allons faire », et ensuite nous présentons cela à la communauté. Il y aura une scène de révision de la communauté.

Posez-moi des questions sur les révisions. Au cours de la prochaine année et demie, nous aurons des entretiens avec le comité de sélection de la communauté afin de déterminer si oui ou non a) nous faisons ce que nous avons dit que nous allions faire, mais b) ce que nous disions que nous allions faire dans notre future stratégie est la bonne chose à faire.

JOHN CRAIN : Au gala ou non.

FEMME NON IDENTIFIÉE : Merci bien. Comme d'habitude, j'aime disposer du temps d'autrui, alors si vous retrouvez un de ces gars, arrêtez-le, posez lui des questions.

JOHN CRAIN : Cherchez des gens avec des drôles de chapeaux. Normalement, c'est nous.

FEMME NON IDENTIFIÉE : Merci bien d'être venus. Et pour tout le monde : au gala, et profitez de votre soirée. Je vous reverrai demain matin, très tôt, enthousiastes et ponctuels.

STEVE CONTE : Avant que tout le monde se lève, dernière déclaration qui n'a rien à voir avec la sécurité et la stabilité. Il s'agit de vous, les gars. Vous êtes vraiment la voix de l'Internet, et le fait que vous soyez là, sans être payés, nous dit quelque chose. Alors, continuez ce chemin, faites ce que vous voulez faire, et faites de l'Internet ce que vous voulez, parce qu'il vous appartient, il nous appartient. Je vous félicite d'être ici. Merci.

[FIN DE LA TRANSCRIPTION]