TORONTO –Panel d'Experts sur la Sécurité de l'ICANN (Forum sur l'abus de DNS)
Lundi 15 Octobre 2012 – 13:30 à 14:45
ICANN - Toronto, Canada

BRAD WHITE: On est entrain de résoudre des problèmes de participation à distance de dernière minute et nous allons commencer. On est près pour commencer. Nous voulons que cette séance soit différente des autres auxquelles vous avez assisté à l'ICANN. On veut que se soit aussi interactif que possible, on veut répondre à autant de question de façon très participative, très déstructuré ; c'est ça qu'on recherche. On a un panel merveilleux qui va venir vous parler de sécurité ; c'est un panel unique, Je vais les présenter:

On a Jeff Brueggeman, le vise président de politique publique pour AT&T et il est responsable de développer et de cordonner les positions de politique publique d'AT&T sur internet. Il dirige les initiatives de politique de coordination et des services d'émergence tels que la sécurité du haut débit, la sécurité du Cloud, le service d'IP.

Je ne sais pas qui c'est le bonhomme à coté de lui. Non ce n'est pas vrai ; c'est le Docteur STEVE CROCKER, le président du directoire de l'ICANN, le conseil d'administration de l'ICANN et le cofondateur de la corporation Shakuro. Il a travaillé sur le développement des protocoles de sécurité internet, c'est à dire du DNSSEC. STEVE est un pionnier de l'internet qui a aidé à établir les protocoles d'ARPANET qui était bien sur la base de l'internet tel que l'on connaît aujourd'hui.

À son coté Jeff Moss, le vise président et l'officier de sécurité en chef ; on le connait très bien pour son travail ; en 1992 Jeff a fondé la communauté de hackers la plus grande au monde et cinq année plus tard, il a changé de casquette, il a changé de coté et il a fait la recherche de sécurité. Il a été nommé pour le département de sécurité interne des États-Unis et fourni son conseil au gouvernement. C'est ça Jeff? C'est vrai? C'est une biographie très longue… j'ai du la réduire ; il a fallut résumer.

Puis on a ici Debbie Monohan, le commissaire des noms de domaine du CCTLD de la Nouvel Zélande. Il est responsable du contrôle de l'espace de noms de domaine et il est aussi responsable des bureaux d'enregistrement et de faire respecter les contrats de service.

Puis nous avons Dan Kamisky qui est un chercheur en sécurité ; c'est facile à comprendre comme ça. Il a toujours prêté conseil à des compagnies telles que CISCO et Microsoft entre autre ; c'est presque 500 compagnies. Il travaillé sur les DNS d'internet et on appel son virus le kamisky bug. C'est l'insecte Kamisky et on le remercie de l'avoir crée ; n'est ce pas? C'est lui qui a provoqué la solution la plus grande pour l'internet de toute l'histoire d'internet.

Puis nous avons Docteur Paul Twomey, notre ancien PDG d'ICANN et le Directeur en chef d'ARGO PACIFIC, un cabinet de conseil international qui aidé à créer les affaires de sécurité d'internet. Il est un ancien président du conseil global de l'agenda d'internet pour tout le monde ; c'est un panel comme j'ai dis très distingué, on veut que cette séance soit aussi informelle que possible. Je vais donc poser les premières questions mais lorsque vous serez près, rapprochez vous des micros.

Nous avons quelqu'un qui représente les participants à distances, c'est Margie ; elle va nous lire les personnes qui participent à distance. Et je voudrais simplement te poser, Steve, la première question pour clarifier un peu. Qu'est ce qu'ICANN a à faire dans la sécurité? C'est-à-dire quel est le rôle de l'ICANN en termes de sécurité?

STEVE CROCKER: Je remercie des questions faciles et simples. Je fais une pause parce que j'essaye de résumer pour ne pas dire que ce n'est pas l'xyz. Le rôle d'ICANN en terme de sécurité se base sur sa mission de cordonner les identifiants uniques. C'est un mot qui inclut mais qui n'est pas limité au système de noms de domaine et la portion de sécurité, qui porte sur ces noms de domaines ; mais ça inclut aussi les adresses et les numéros de signes, le système de numéros autonomes et ils ont publié le Protocol de paramètre ITF et notre participation dans le marché avec le gTLD, les registres et les bureaux d'enregistrement porte sur la cohérence et sur la coopération entre ces deux. la sécurité est un mot important et ça comprend plein d'aspects et les gens attachent des significations importantes à ces aspects et je pense que ce n'est pas un terme assez précis parce que sa inclus le phishing, le hameçonnage, l'extorsion, l'espionnage et pleins d'autres problèmes que l'on a. il ya des gens qui se servent des SPAM, comme mesure pour faire l'intrusion, comme moyen pour être des intrus, faire des abus et cela bien sur provoque des sentiments dans le public. Notre problème est très séré là-dessus ; ce n'est pas large. On travaille sur la stabilité des opérations de serveurs racines ; c'est très important parce qu'on travaillé sur la qualité et la précision des informations de zone racine. C'est très spécifique et c'est un secteur qui est tout petit. En faite on doit travailler aussi sur

l'opération du système de noms de domaines ; voilà pourquoi on soutient le DNSSEC. On attache une grande importance au système d'opération des registres et des bureaux d'enregistrement et on a une quantité limité de fraude d'abus dans ce domaine. Jeff Moss va sans pouvoir plus nous dire là-dessus.

BAD WHITE: Ce qui me mène à la prochaine question, JEFF. On se parlait avant la … le début de la séance et on discutait de la mission d'ICANN dans le rôle de la sécurité DNS et quelle est la mission qu'on ressent avoir. Est-ce qu'on peut le discuter?

JEFF MOSS: Oui bien sur. A l'ICANN, la communauté nous soutiens dans tout ce qu'on fait. On a un accord que l'on vu dans le SSR, le document que l'ICANN vient de publier. On croit que c'est un document bref, concis qui montre le rôle d'ICANN dans la sécurité dans SSR ; cela a été publié et diffusé à travers le forum, on va tenir compte des commentaires de la commuté. Mais, ICANN pense que son rôle en fait est conçu de différentes façon, selon quel membre de la communauté y réfléchi. C'est dire qu'ICANN cordonne le système de nom de domaine global et donc ce qu'importe est ce qu'est le système de mon domaine. On a des pays qui n'ont pas de zone racine et on voit qu'on a une interruption de service dans ces pays. Peut être que l'ICANN va aller les voir si on a ce genre de problèmes. On a des opérateur de racine, or les problèmes ne s'arrête pas avec l'ICANN ; ça s'arrête aux zones racines. Donc plus on clarifie le rôle d'ICANN, mieux ça fonctionne et c'est mieux pour la

communauté, pour qu'elle sache mieux quel est le rôle d'ICANN pour générer d'avantage l'intention des gouvernements. Plus on le clarifie mieux on va fonctionner ; parce que le plus ambigüe, le plus difficile c'est de travailler non seulement pour le GAC.

BRAD WHITE: Oui. On parlait tout à l'heure des anonymous, vous regardiez la télé en février n'est ce pas? Tu as mentionné un point qui me semblait très important ; tu disais que l'on parlait d'une menace, qu'on devait contacter quelqu'un à travers le téléphone et qu'on devait en quelque sorte détourner l'internet.

JEFF MOSS: Oui oui, c'est ça. Mais ça ne va pas fonctionner comme ça. Lorsque l'on commence à chercher qui c'est l'internet, il ya des gens qui ont comprit qu'ICANN étaient internet et d'autres disent qu'on est des coordinateurs internationaux. Je parlais des opérateurs de la zone racine et on m'a dis: est ce qu'on ne devait pas être là? Oui oui, je ne vous envie pas on m'a dis que vous avez écrit que vous êtes les personnes qui coordonnent l'internet. Mais moi je l'ai écrit nulle part en fait. Donc ce que je fais c'est de mon mieux ; je vais faire de mon mieux pour que mon service fonctionne. Mais si j'échoue, j'ai fais de mon mieux. Si c'est vous qui échouez, c'est écrit sur votre papier de contrat ce n'est pas moi. Alors c'est une situation un peu intéressante.

BRAD WHITE: PAUL, vue que tu as été le PDG, es-ce que tu as vu des incidents de sécurité qui tiennent compte des modifications de l'ICANN? Les attentes, les modifications dans les attentes?

PAUL TWOMEY: En fait, je pense que depuis que l'ICANN existe, l'interaction avec les opérateurs de la zone racine a été une relation d'engagement et de coopération ; je pense que le défi était de comprendre l'intension du gouvernement en 99-2000 et c'était beaucoup plus participatif que ça pouvait l'être. On était plus engagé au rôle de coordination et pour les opérateurs de la zone racine, pour qu'ils se rapprochent du processus de l'ICANN, ils ont dû le faire pour un nombre de raisons. C'est en premier lieu pour ce que Jeff vient de dire mais aussi pour l'infrastructure que l'on devrait avoir ; une espèce de système de sauvegarde pour que si on a des crises, on puisse les maitriser. On doit faire que toutes les personnes qui participent comprennent ce que résilient veut dire. Donc la question qui a été publié pour le commentaire public de l'ICANN, pendant qu'on fait la transition de la zone racine, on a beaucoup travaillé avec les opérateurs de la zone racine en fait et je pense que c'est essentiel.

JEFF MOSS: Oui, j'aurais voulu que cela se fasse dans notre temps, dans notre délai et pas en urgence.

BRAD WHITE: Vous dites comme-ci c'était inévitable et on a ce sens que c'était inévitable.

JEFF MOSS: Je pense que ce n'était le cas que deux fois dans le passé et c'était quelque chose qui s'était passé simplement et pas une procédure… on a acquis une autre compagnie par exemple et ça a aidé. Si on imagine une autre acquisition de compagnie, on pourrait se dire, bon moi, c'est fait, je prends ma retraite, je ne veux plus travailler, je veux vendre ma compagnie à travers ebay ; donc ça devrait être quelque chose de prévisible.

BRAD WHITE: Debbie, quel est à ton avis le rôle de l'ICANN dans la sécurité?

DEBBIE MONOHAN: En fait, l'ICANN n'a pas un rôle et la sécurité s'améliore à mesure qu'on travaille sur les ccTLD et ce qu'on cherche c'est d'avoir une coordination dans toute l'organisation. Je pense que l'ICANN a une bonne position pour tenir compte des points de vue des différentes parties prenantes à partir de son modèle et des documents et je pense que le ccTLD peut mettre en place toutes ces modifications parce qu'ils vont se servir des ccTLD selon les codes de pays.

Lorsqu'on discutait des pays qui n'avaient pas de zone racine, on a traité du sujet avec l'ICANN et cela inclut l'ICANN si vous voulez et le fait qu'ils vont devoir assurer la sécurité des DNS.

Lorsque les personnes s'enregistrent, ils ne savent pas qui ils peuvent aller voir pour savoir qui c'est qui contrôle ce système. Donc à mon avis, l'un des rôles de l'ICANN est de voir si le document et les endroits où cela fonctionne peuvent être bien faits. Les ccTLD peuvent atteindre ce point parce qu'on est tous dans un même espace et c'est très souvent qu'on essaye de les résoudre en très peu de temps. Donc on veut savoir qui c'est que l'ICANN est vraiment. Donc, ils n'ont pas un rôle vraiment établi mais on se sert de bases de données pour le savoir selon les circonstances. Donc on ne doit pas être alarmiste mais on doit trouver la façon dont on veut fonctionner.

BRAD WHITE: Dan, je veux savoir quel est ton point de vue. Quel est, à ton avis, la plus grande menace pour les DNS?

DAN KAMINSKY: Il ya plein de gens qui veulent modifier le système de DNS ; ce n'est pas que les hackers. Ce qui me préoccupe, c'est l'augmentation de refus (dénie) de service, de ce genre d'attaques ; on travaille dessus depuis une décennie. On essaye de remettre ce problème et maintenant l'autre coté est entrain de travailler dessus aussi. Donc c'est devenu une course très rapide et c'est une question d'échelle. Entre les attaques de dénie de service que j'ai vu augmenter de façon exponentielle et les concessions entre les bureaux d'enregistrement et les registres, ce que je vois de plus en plus, est qu'on applique énormément de force à une échelle qui est beaucoup plus grande que ce qu'on aimerait qu'elle soit. Donc, ça veut dire qu'on désire avoir une indépendance dans l'espace ;

on a nos petits secteurs et c'est là où on se sent et le reste des gens pourrait nous conseiller s'ils voulaient le faire mais c'est notre espace. Et ce système doit fonctionner pourvu qu'on ait des acteurs avec beaucoup de pouvoir, qui fassent une force et qu'on soit très très puissant. Si on ne l'est pas, ça va nous revenir, ça va nous ramener en arrière. C'est ce que je voudrais que l'ICANN fasse, que ce soit le rôle de l'ICANN. On a besoin d'avoir une coordination. La réponse à Anonymous, comme je le disais à Jeff tout à l'heure, le fait de menacer le système de DNS pourrait être leur action la plus puissante. C'est comme un vaccin ; on n'a pas de menace mais est ce que ça a créé des réponses d'immunité. Le DNS est beaucoup plus stable grâce à une menace synchronisée où il n'y avait pas vraiment de menace. Je suis très… j'ai de bonnes attentes, j'ai des espérances et on est prêt à répondre aux menaces en tant que groupe coordonné ; c'est ça mon point de vue sur la situation en ce moment.

BRAD WHITE: Parlons de la coordination. Après avoir commencé à travailler avec l'ICANN, ils vous ont aidé à configurer ce système ; et pour moi, lorsque j'ai intégré ce monde, que je l'ai rejoint, c'était merveilleux de voir que tout le monde travaillait ensemble contre cette menace. Est-ce que ce serait le cas pour la défense contre ce genre de menace?

DAN KAMINSKY: Je pense qu'on n'a pas de modèle. On est coincé ensemble, on n'a pas d'alternative. On devrait trouver un mode pour gérer ce genre de menace. On doit travailler ensemble pour régler ces problèmes.

On peut essayer de résoudre les attaques que l'on reçoit mais aucun registre individuel, ni bureau d'enregistrement individuel, ni organisation indépendante ne peut le faire toute seule. On doit travailler de façon coordonnée et cette coordination devrait se faire avant que l'attaque ne commence.

JEFF MOSS: En fait, la menace anonymous… et dans l'avenir, les futures menaces vont devoir être traitées de la même façon. Moi, ce qui ne me laisse pas dormir le soir est ce qui pourrait se passer. Lorsqu'on a eu la menace d'anonymous, on ne savait pas quel était le flux qu'on allait recevoir de tout le monde et quel était le seuil. C'était 132 GB à l'époque ; c'est un flux qui est assez important. Mais la semaine dernière, on a eu 212 GB. Donc on est passé de 132 à 212 en moins d'un an ; je n'aime pas moi ces résultats. Je ne sais pas comment vous pouvez vous défendre d'une menace de ce genre à moins que vous ayez beaucoup de débit, de connexion pour pouvoir trouver ces flux parce que sinon on aura du mal à les résoudre. Tous les opérateurs et leurs serveurs sont dans un même pays en général et même dans une même ville donc si c'est dans votre communauté ou dans votre pays, vous serez menacé pour limiter ce genre de menace autant que possible. Donc j'aimerai davantage voir une coordination autour d'une stratégie unifiée pour limiter à des flux de 132 - 212 GB.

ERNIE DANIELS: Bonjour, je viens d'Afilias. On est préoccupé par la quantité d'attaques de dénie de service qui sont de plus en plus nombreuses et je pense

qu'il ya plusieurs facteurs en fait qui sont en jeu dans ce cas ; on les a vu dans le passé. Au tout début, le dénie de service était dû à une défaillance qu'on a découverte et la solution était de mettre un patch au TCP et de continuer de travailler. Cette stratégie est devenue plus difficile avec les botnet parce que c'est beaucoup plus difficile d'identifier toutes les machines et de les patcher. Mais on a connu ce problème depuis quelque temps déjà ; on sait qu'il existe. C'est au delà d'une défaillance du système que l'on puisse réparer. En fait ça a créé à la conception du protocole ; si on s'en sert de la façon dont on l'a créé, on pourrait avoir une magnitude beaucoup plus grande que ce qu'est le flux et je sais que l'on travaille dessus. Je ne sais pas si d'autres protocoles vont avoir cette défaillance subliminale qui n'est pas vraiment visible et pourrait être latente. Donc je ne sais pas si on va pouvoir traiter le dénie de service à travers les défaillances des protocoles.

DAN KAMINSKY: Le DNSSEC n'est pas particulièrement spécial pour son élargissement, son amplification ; mais ce qu'on voir est que lorsque cette amplification est une réalité, ça n'attaque pas le DNSSEC mais ça attaque le DNS directement. Ça ne passe pas par le DNSSEC. Et en définitive, notre solution pour les attaques de dénie de service était d'avoir davantage de débit que ce que les autres ont. Nous on a l'argent, on a les moyens qu'ils n'ont pas ; donc on force davantage de débit pour les battre. Au début, on a eu 212 GB comme flux et en fait ça n'échelonne plus ; c'est ce que je vois et c'est ce que je verrai la prochaine décennie. On n'a pas tout le monde qui travaille ; quatre, cinq ou six fois à la vitesse à laquelle nous travaillons ; alors est ce qu'on voit

des protocoles, est ce qu'on voit des réseaux qui sont entrain d'être restructurés. Ça se passe de façon technique, mais aussi au niveau des politiques. Les gens vont être d'accord lorsqu'on dit qu'on va devoir rechercher comment traiter les trafics des spoofs, comment communiquer avec les peers et combien c'est pertinent de traiter les problèmes. En fait, vous savez, l'attaquant passe par ces sujets. A présent, on ne sait toujours pas ce qu'ils essayent de faire ; on sait qu'ils ont décomposé les problèmes et qu'ils ont essayé de les maintenir autant que possible. Mais ce n'est toujours pas ce qu'ils veulent.

BRAD WHITE: Steve, tu veux ajouter quelque chose?

STEVE CROCKER: Je suis d'accord avec ce que Dan a dit. Dan, tu as mentionné le fait de réfléchir à ce que ça ne dépend pas des DNSSEC et que ça attaque simplement le DNS. Le mécanisme qu'on est entrain d'explorer pour faire face à ces attaques est les adresses sources…fausses sources. Pour les résolveurs DNS, lorsqu'on a une adresse qui n'est pas vraie, qui est fausse, notre cible qu'on essaye d'attaquer va être mitigée ; on a déjà accordé qu'on va travailler sur les adresses sources pour mitiger ce problème et qu'on ne devrait pas permettre qu'un utilisateur ou une machine envoie un paquet qui traite de mots ou de fausse publicité. J'ai vu que c'était décrit en tant que problème en 1998, on fait de plus en plus attention la dessus et ce n'est pas… mais on essaye de le communiquer aux fournisseurs internet et on va travailler sur

l'évaluation du point où on en est avec le processus et où on n'en est pas.

BRAD WHITE: Jeff.

JEFF MOSS: Je n'ai rien à ajouter sur les problèmes techniques mais j'aimerais dire que ces attaques créent aussi des préoccupations politiques qu'on doit connaitre, desquelles on doit être conscient et le pire des cas pourrait être que le gouvernement appelle internet pour résoudre ce problème. On était conscient du fait que l'ICANN ne pouvait pas excéder son rôle et ce qui nous préoccupait est que pour les gouvernements en particulier la sécurité est un problème plus important pour eux. S'ils ne comprennent pas ce qui se passe aujourd'hui et potentiellement essayer de voir notre rôle gouvernemental pour les partenariats globaux etc. donc je pense qu'on doit luter contre les problèmes techniques mais c'est aussi l'occasion de montrer qu'on manque de contrôle centralisé mais que ce n'est pas une faute, c'est un bénéfice pour la façon dont internet a été conçu. Ce n'est pas simplement qu'on doit être des coordinateurs formels mais qu'on doit combiner les parties techniques et les aspects de l'infrastructure qui peuvent aider à résoudre ces problèmes.

PAUL TWOMEY: Je peux ajouter quelque chose à ce qu'ils viennent de dire? Il faut agir selon les époques ; cette semaine, j'ai vu que le secrétaire d'état à la

défense des Etats-Unis a dit, il ya deux ou trois jours, que dans leur pays, ils avaient des infrastructures infectées et qu'ils allaient donc lancer un système tout nouveau pour lutter contre cela. Je pense que c'est un sujet pressant pour la communauté ICANN et que l'ICANN va devoir travailler sur l'approche multipartite pour détourner les zones racines qui n'ont pas souffert de modifications et des problèmes sur les DNS et ce qui porte sur le conformité, etc. On doit être claire par rapport à notre rôle parce que ce qui me préoccupe c'est qu'un jour, on pourrait se retrouver dans une situation ou un conflit va produire un conflit en ligne. Les gouvernements sont préoccupés par les contenus en général ; mais vu le cyber-espionnage et les conflits, il est absolument nécessaire que l'on travaille sur l'infrastructure du réseau. Ce qui me préoccupe moi est que le modèle communautaire de l'ICANN se centre sur les parties prenantes, sur la communauté et la transparence. Donc, il faut être clair sur ce problème pour pouvoir éviter la gestion de la crise ou alors si ce n'est pas clair, lorsque la crise commence pouvoir la résoudre plus facilement.

BRAD WHITE: Ca m'étonne un peu que le genre de conflits conventionnels pourrait être suivi par un conflit en ligne.

DEBBIE MONOHAN: Ce n'est pas spécial pour les DNS et je pense que c'est important de comprendre et de clarifier de quoi il s'agit. Donc lorsqu'on me dit qu'il ya des pays qui ont des noms dans un même pays donc un seul lien à partir duquel ils téléchargent l'information ; et si cette connexion

échoue, le pays en entier sera déconnecté. Donc ce qui est important pour moi est de savoir qu'est ce qui a trait au DNS et qu'est ce qui ne l'a pas parce que dans l'infrastructure même, on va travailler sur certains aspects. Donc c'est comme une espèce de réseau normal ; on ne peut pas garantir que dans toutes les rues de la ville il sera facile de conduire et qu'il sera aussi facile que dans une autoroute aux Etats-Unis. Bien-sur que ça ne devrait pas l'être même et il y'aura des situations où l'on atteint ce genre de scénario en Afrique et donc on devrait comprendre ce que sont les DNS et qu'est ce qui n'appartient pas au DNS. Qu'est ce qui a trait à quoi lorsqu'on parle des protocoles, on doit savoir de quoi on parle ; lorsqu'on parle des attaques. On ne peut pas dire que dans le monde mobile, par exemple la veille de noël tout le monde attend ses parents et 10% se connectent et s'effectue un attaque ; bien sur que non. 90% n'a pas pu se connecter dû à une attaque ; ce n'est pas qu'ils ne se connectent pas pour parler à leurs familles parce qu'il ya une attaque mais en fait on ne sait pas ; ça pourrait l'être. Les protocoles garantissent une connexion de point à point, ça appartient au réseau d'internet et c'est intégré dans le protocole. On devrait savoir si on a ce Switch dans le paquet ; on ne doit pas mettre autant de pression pour faire que ça ne s'interrompe plus. Les gens ont à comprendre ce point. Ce n'est pas qu'on va résoudre le problème, chaque problème qu'ils ont ; il faut traiter et faire la distinction entre cela ; c'est très important d'être transparent sur ce qui est possible, ce qui ne l'est pas et sur ce qui a trait au DNS et sur ce qui ne l'a pas. Voilà.

DAN KAMINSKY: J'étais à une réunion avec deux cent ingénieurs, je me souviens que je leurs ai demandé combien parmi eux écrivaient ou codifiaient des

logiciels qui dépendaient du DNS et de deux cent personnes, il n'ya que deux qui ont levé les mains. Et je dis, je vais paraphraser combien parmi vous avaient des logiciels qui espèrent avoir une chaine de texte pour vous rendre une adresse IP pour pouvoir se connecter au réseau? Et puis 198 ont levé la main. Tout a trait au DNS ; tous les problèmes portent sur les DNS. C'est la base sur laquelle on construit les protocoles qui espèrent pouvoir communiquer le long de la communauté et au delà des limites de la communication ; ces protocoles peuvent le faire grâce au DNS qui leurs donnent la capacité de le faire. En fait ce qu'on voit, c'est qu'on voit beaucoup d'acteurs, des hackers mais pas seulement eux qui manipulent les DNS et croient qu'ils peuvent manipuler tous ces protocoles encore plus larges. Ça pourrait être dû a des raisons de cybersquattage ou parce qu'un adolescent veut s'amuser ; on a plein de raisons pour essayer de corrompre internet et les DNS sont un bon point pour aller travailler la dessus. C'est un bon point d'attaque. Imaginez que toute la connexion d'un pays se déconnecte ; ça ne veut pas dire que tous les sites du pays sont tombés ; les sites pourraient être stuqués à un niveau global à travers un système de caste ou peut être qu'ils sont toujours en ligne mais ça… personne ne peut trouver ces adresses. Donc ça marque un point de changement où l'on va repenser aux attaques. Si vous attaquer ici, vous aller tout casser. On voit qu'il ya plein de gens qui ont provoqué des changements très intéressants sur internet. On a quatre standards qui sont la sécurité, la souveraineté, la confidentialité et les attaques ; ce sont des forces qui essayent de faire des modifications, mais on a une force principale qui unit toutes les personnes dans cette salle et à mon avis c'est l'accessibilité. On construit quelque chose de merveilleux qui va continuer de fonctionner. C'est remarquable combien de gens

reconsidèrent l'accessibilité de cette histoire ; des gens qui ne sont pas dans cette salle.

RICK WESTON: Bonjour, je veux poser une question mais je veux en même temps vous remercier de prendre le temps d'organiser cette séance. Ma question est venue plusieurs fois dans le monde de la cyber-sécurité. Je pensais à la capacité en ligne pour les feuilles de connectivité ; ceci, je sais fait peur à beaucoup de gens. L'ICANN est dans une position unique pour coordonner les points d'internet et pour le rendre stable et confiant ; pour le maintenir en ligne. Je pense que si on peut passer de sécurité à santé, vous allez voir qu'on a beaucoup plus de… on attache beaucoup plus d'importance au système dans un endroit qui est bon pour la santé. Vous l'avez vu, on a plein d'autres moyens, il ya plein d'autres façons de faire fonctionner internet, de le considérer aux yeux de la communauté globale, indépendamment du statut global ou national. Donc ce que je voudrais voir est la création d'un entourage qui rend possible la santé de l'internet ou comme l'OMS. L'OMS travaille avec la communauté de la santé parce qu'ils ont des relations et c'est aussi ce que l'ICANN a. je pense que c'est sa valeur pour la communauté globale et pour nous éloigner un peu de la conversation de sécurité, je pense qu'on devrait penser à ce qui est salutaire pour les populations. Merci.

SIMON MCCALLA: Bonjour, je suis Simon Mccalla de Nominet (Royaume Uni). J'ai une question pour le panel. En général on parle de DNS dans l'industrie ; et on est des experts la dessus et on parle de résolution des problèmes. On

a travaillé avec les fournisseurs internet du Royaume Uni et on a essayé de résoudre les problèmes de données des consommateurs ; mais notre problème dans ce débat est qu'on perçoit un manque d'attention et on ne comprend pas très bien quel est le trafic. Donc Jeff, je pense que j'ai une question pour toi ; c'est comment on résout le problème pour que les hackers régulent la santé de leurs DNS sans attaquer la confidentialité.

JEFF MOSS: Oui, c'est un grand problème. Ce n'est pas seulement pour des problèmes de santé mais pour le transport de l'information, pour améliorer le transport entre le secteur privé, les compagnies et le gouvernement. On essaye de traiter ce problème avec la protection structurelle pour que ce soit clair que si on va aider dans un problème personnel dans votre ordinateur, sur votre ordinateur et avec votre service, on va devoir le faire dans la mesure du possible. Mais on a des menaces pour les informations, les flux de données qui peuvent être partagées sans être une préoccupation personnelle ou individuelle ; mais en même temps le problème des concessions par rapport au traitement des menaces et en même temps préserver la confidentialité, la vie privée des gens en ligne. La meilleure façon de le faire est d'avoir une solution transparente pour qu'on n'ait pas de surprise par rapport à ce que les fournisseurs internet font.

BRAD WHITE: Jeff, je voudrais te poser une question par rapport aux efforts collaboratifs que l'on a faits. Lorsqu'on a eu une menace, on voit qu'il ya

une relation entre les gens qui travaillent sur les relations publiques. Vous parlez tout le temps de transparence ; bien sur que c'est important mais comment est ce que vous trouver l'équilibre entre les bénéfices de la transparence et les menaces?

JEFF MOSS: Ce qui me préoccupe est… je pense toujours aux gens qui travaillent dans l'aspect politique et dans la politique, si on a des défaillances du serveur de noms, bien sur on peut trouver une solution mais on ne sait pas quelles sont les conséquences secondaires avec les gens politiques si ça aux gens à dire je ne fais pas un travail assez bon ou si on a un autre moyen de prendre ces sujets au sérieux. Ce n'est pas que je réponds à votre question directement mais on peut changer un peu ; on voit des situations un peu différentes où on considère que ce sont des problèmes techniques et qu'on n'a pas besoin des gens des relations publiques mais avant ils étaient très utiles.

JEFF BRUEGGEMAN: On travaille sur un effort dans tous les secteurs pour pouvoir coordonner nos efforts. J'ai aimé l'analogie de la santé pour que la machine fonctionne bien mais aussi pour qu'on ait les meilleures pratiques les plus sures sur internet. On a des gouvernements qui travaillent dessus avec les fournisseurs internet et les personnes qui développent des navigateurs internet ; donc on pense, même si on ne peut pas les résoudre tout seul, on a des compagnies ou des endroits où on atteint les consommateurs et peut être qu'ils ne sont pas très bien informés ; une partie de leur travail est de nous dire quels sont les cinq

point qu'on devrait remplir et ce n'est pas facile pour nous de leurs expliquer tout cela. S'ils veulent prendre des mesures, ils ne savent pas toujours comment le faire.

BRAD WHITE: Paul?

PAUL TWOMEY: Je suppose que la crise politique porte sur la transparence des processus. Je ne sais pas s'ils ont beaucoup appris le long des années ; donc si on prend l'exemple des conflits, une partie du traitement de la crise va porter sur la confidentialité et le fait de ne pas être transparent par rapport à ce qu'on fait. Ce qui est important est que les gens sentent qu'ils savent ce qu'est le processus et comment il va être suivi ; c'est ça le fait d'être transparent. On a des différences dans les interactions parce qu'ils veulent voir des communications, des relations publiques ; mais en même temps on devrait avoir une transparence par rapport à qui c'est qui participe, qui est engagé et c'est une valeur essentielle. Je pense que c'est commun à toutes les communautés de l'ICANN et pour la sécurité des DNS. Ce genre de problème sera pire à chaque fois si on ne le traite pas. Par rapport à la réponse des 200 ingénieurs, c'est une spirale, et on l'espère, qui avancera vers le bas et non vers le haut ; donc on devra trouver une bonne réponse au moment de crise et on doit établir la différence entre la transparence et la crise et la différence pendant la crise.

BRAD WHITE: Debbie.

DEBBIE MONOHAN: Je pense qu'on doit trouver des solutions au moment même de la crise. Ce qu'on a fait lors de la crise était de bloquer l'administration de noms sur la liste, puis on a trouvé un processus pour résoudre les problèmes avec les bureaux d'enregistrement et les registres ; avec les registres légitimes on avait bloqué des noms et on a trouvé une façon de diffuser un nom pour qu'il soit publié encore une fois. On doit travailler avec les fonctions internet, on pourrait dire on va tout fermer mais on a la responsabilité de faire fonctionner les ccTLD avec leurs chaines correspondantes ; donc le problème il me semble était de trouver les solutions et on peut trouver plein de solutions de façon innovatrice.

BRAD WHITE: Oui, Dan?

DAN KAMINSKY: Je pense que le centre des relations publiques et de la sécurité doit être d'agir ; on ne peut pas annoncer des mesures et ne rien faire. Si c'est ce qu'on va faire, l'attention des gens va être gâchée ; on gâche l'occasion de faire quelque chose. Si vous voulez que les gens agissent pour qu'internet soit plus sécurisé, plus sûre comme ambiance, on doit leurs dire quoi faire ; installer ce logiciel, faites cela. Si c'est juste pour les informer, je pense que ce n'est pas saisir le temps.

BRAD WHITE: C'est d'être proactif et pas réactif.

DAN KAMINSKY: Oui, ce n'est pas simplement d'annoncer les problèmes qu'on a ; il ne s'agit pas de dire allez voir ce problème sur lequel on travaille. Je pense que la sécurité et les relations publiques, il est important de leurs dire qu'est ce qu'ils peuvent faire ; et s'ils sont d'accord avec ce qu'on dit, on leurs dit ce qu'ils peuvent faire. C'est-à-dire, on fait cela, si vous êtes d'accord faites cela. C'est ça mon point de vue.

BRAD WHITE: Jeff.

JEFF MOSS: Je pense qu'on doit le faire et avec les consommateurs et avec les gouvernements. Je pense qu'il ya beaucoup de crainte et personne ne sait quoi faire et ils s'inclinent à ne pas bien agir parfois. Donc, peut être que la communauté technique et les personnes qui opèrent sur les registres n'ont pas bien travaillé pour le faire. Qu'est ce qu'on peut faire? Voyons qu'est ce que vous devriez faire que vous n'êtes pas entrain de faire? Et d'articuler ces idées. Je suis d'accord avec Paul ; je pense que le risque est de plus en plus important et que le niveau d'attaques augmente. On va devoir prendre des mesures et donc je pense qu'on devrait classer les personnes pour qu'elles prennent les mesures.

RICK WESTON: Je pense qu'il est important qu'on apprenne d'autres industries par rapport à la façon d'agir et je ne suis pas d'accord avec toi Dan. Si vous voyez les problèmes de santé qu'on a eu au monde depuis qu'on a appris à se laver les mains ; par exemple, on a des problèmes avec le SIDA et on a discuté pendant des années pour apprendre à le résoudre. Avec toutes les maladies qu'on a eu c'était pareil. Il faut considérer ces expériences comme façon de traiter des situations similaires. Ce n'est pas des problèmes qu'on continue d'avoir mais ça affecte une population entière, la population mondiale. Merci.

DAN KAMINSKY: C'est une analogie qui est très intéressante et ce que j'aime bien c'est qu'elle n'est pas en opposition avec ce qu'on dit ; mais c'est un problème différent en fait. On a à peu prés prohibé, interdit la guerre biologique ; on pourrait être entrain d'explorer les gènes et les bactéries d'autres gens. On ne peut pas me faire ; mais pour la sécurité, les gens disent qu'on envoie un code fou tout le temps. Donc ce sont des types d'ennemis différents.

BRAD WHITE: Monsieur vous avez beaucoup attendu.

MIKEY O'CONNOR: Merci. Mon nom est Mikey O'Connor, je suis un des co-présidents de DSSA ; c'est le groupe d'analyse et de stabilité des DNS. Vous savez comment il a été créé donc je ne vais pas le redire, mais j'aime bien ce qui se passe ici dans cette salle. J'adore les commentaires que Steve a

faits au début. Je veux dire, il ne faut pas faire ce que l'ICANN ne fait pas, il faut décrire ce que l'ICANN fait. J'ai bien aimé que Paul parle de coordination, de transparence, de penser et réfléchir en avance ; j'aime tout ce que Dan dit en fait.

Mais je voudrais détourner un peu ce sujet et passer au document qui a été présenté pour préparer cette réunion ; c'était la déclaration révisée pour l'accord de l'ICANN. Je ne l'ai pas aimé autant ; je suis membre du regroupement de fournisseurs internet et je rencontre des gens qui ne sont pas agréables parfois. Je ne vais pas le répéter car c'est beaucoup plus long que l'accord de déclaration ; mais je pense qu'on doit s'améliorer, améliorer précisément ce document. Il me semble que le rôle de l'ICANN et la confusion qu'il ya autour est toujours le centre de la discussion. On se demande ce qu'on peut dire par garantir par exemple parce qu'on peut garantir de plein de façons différentes. Ce n'est pas quelque chose que l'on peut résoudre dans une réunion telle, mais j'aime bien qu'on en discute et j'encourage ce groupe à la table à travailler dessus. Je sais que vous avez des problèmes techniques qui sont très importants mais on doit commencer à penser aussi à la façon dont nous travaillons ensemble ; qui fait quoi dans l'écosystème des DNS? Merci.

BRAD WHITE: On peut répondre peut être. Est-ce que vous trouver qu'on n'a pas de clarté en ce moment? Jeff, tu te reposes? Je ne sais pas ; tu veux parler?

DAN KAMINSKY: Je pense que Jeff a tout dit, il a dit je ne vais pas répondre. Je pense que Mike a raison ; les mots et les règlements intérieurs sont très bons pour les moments où ils ont été écrits et je n'étais pas là lorsque c'était fait. Mais j'imagine qu'ils sentaient que c'était sensé ; il souhaitait poser des questions et ils répondaient on va voir comment ça fonctionne ; on va attendre jusqu'à ce que ça se passe pour le revoir. Et je pense que le moment de les réviser et de les reconcevoir est venu. Et comme j'ai dit, l'ICANN n'est pas le seul opérateur dans l'espace ; on a d'autres gouvernements, dans l'industrie ; c'est ce qu'on appelle les partenaires iStar. C'est les registres régionaux d'internet, les opérateurs racines.

ALEJANDRO PISANTY: Bonjour. Je suis Alejandro Pisanty, je viens de l'université nationale du Mexique, l'UNAM et l'ISOC Mexique. Vous m'entendez bien? Au début de cette année, Jeff Brueggeman a créé un panel et il est venu parler avec moi, avec un groupe de parties prenantes pour s'assurer que l'ICANN, son équipe de révision de stabilité et de résilience (et de consensus) travaille bien. Pour moi c'était bon ; mais cette discussion n'est pas intégrée ici comme un point sur lequel on aura avancé. Au lieu de parler de sécurité, j'aimerai qu'on parle d'un panorama plus intégral de gestion des risques qui existent bien sûr. Ce n'est pas que je veux me plaindre parce que mon équipe faisait partie de cette rédaction ; mais je pense qu'on devrait continuer d'avancer et l'ICANN se trouve dans cette situation de guerre asymétrique ou conflit asymétrique. Tout le monde veut ou cherche à ce que l'ICANN ne prenne pas de mesure ; mais quelque chose doit être fait. N'est ce pas? On voit plein de personnes qui pensent à l'ICANN et se demandent quel est le rôle de l'ICANN? Parce que c'est grâce à ce doute qu'on est arrivé à ce point là et les

serveurs, par rapport à ce que Dan disait, ont des DDOS énormes. L'ICANN ne doit pas se mêler du travail des fournisseurs internet, des opérateurs de réseau, des bureaux d'enregistrement. Est dès qu'un DDOS (attaque par dénie de service) a laissé sans connexion plein de serveurs, même si c'était depuis un ré de chaussée, il va y avoir un impact. Les gens vont se demandé: c'est qui l'ICANN? Ils sont où? Est ce qu'ils sont prêts à agir? Donc je voudrai avoir un rapport, un compte rendu par rapport aux avancées que vous avez faites là-dessus et puis pour la gestion de risque, pour toutes les couches (même dans les sphères politiques). Je pense qu'on devrait avoir, j'aimerais bien entendre le panel dire jusqu'où ou combien le risque a augmenté pour les abus massifs ; c'est des aspects qui incluent les dommages politiques ou le préjudice politique pour l'ICANN. Combien est ce que le risque a augmenté ce dernier weekend? Combien est ce que les annonces éveillent l'intérêt de certains groupes qui voudraient attaquer les infrastructures de l'ICANN?

JEFF BRUEGGEMAN: J'aime bien ton point de vue par rapport à la gestion de risque. Ce que j'ai demandé était quel était le débit auquel on s'attendait. Vous avez établi une base et si on ne s'accroit pas en capacité. Je vais reprendre l'exemple de Paul et on va voir si on a l'échelle nécessaire. Je ne sais pas si on a trouvé la solution technique sans ajouter de débit comme Dan a dit et je voudrais trouver une solution. Mais si c'est le monde dans lequel on va vivre, on voudrait savoir quelle est la situation normale? IPv6 peut être traitera davantage de monde, ils vont télécharger des sites plus rapidement. Ces dernières années, on a entendu dire qu'on a une croissance de trente pourcent ; mais ceci n'est pas à la racine. C'est

que les logiciels dans le réseau font, génèrent davantage de demandes. Je vois que vous hocher de la tête, mais on a une croissance de deux numéros, deux chiffres dans ce système, dans ce genre de problème et on n'entend pas parler d'habitude des croissances que l'on espère avoir dans l'avenir. Est-ce que ce sera toujours le trente pourcent de la capacité. On ne sait pas ce que va devenir le nous avec la croissance. Personne ne s'exprime la dessus parce qu'on ne veut pas que les attaques et les hackers sachent quelles sont les limites de notre croissance.

BRAD WHITE: Jeff?

JEFF MOSS: Oui, je pense qu'une partie de nos recommandations portaient sur la nécessité de structures et de processus de l'ICANN pour pouvoir agir. Le comité de directoire est une bonne mesure pour commencer à travailler là-dessus. Il faut qu'on puisse agir, qu'on ait les personnes appropriées pour le faire, mais on doit l'intégrer à la façon d'agir de l'ICANN pour qu'on puisse le faire avec les processus nécessaires et où ce serait nécessaire.

TOM DALY: Bonjour, je suis Tom Daly, le scientifique en chef pour l'opérateur DNS. J'aime bien ce que vous avez dit jusqu'à présent ; vous vous centrez sur les problèmes sur lesquels je pense qu'il faut se centrer. Mais je voudrais dire que l'un des avantages que nous avons qui est ignoré

d'habitude est le fait de pouvoir faire des échanges ; et si on revient à l'analogie de la santé mondiale, ce qui est bon d'avoir des attaques de 212 GB c'est qu'on peut savoir d'où ça vient et comment et résoudre ces problèmes. Mais j'aimerais bien que le panel parle de ces nouveaux facteurs qu'on a vu ces derniers mois ; c'était les attaques envers les registres et les bureaux d'enregistrement eux même parce que c'est un problème beaucoup plus important pour moi. Parce que si on a une population aussi grande qu'elle l'est, on ne sait pas qui c'est qui pourrait nous attaquer et qui ne le ferait pas en termes de DDOS par exemple. Merci.

DAN KAMINSKY: Je l'ai mentionné tout à l'heure, c'était lors d'une réunion avec l'ICANN ; j'ai dit que le bureau d'enregistrement et les registres vont être attaqués sans doute et ce sera un problème de plus en plus important et on ne m'a pas aimé, on n'a pas apprécié que je dise cela lors de cette réunion. Mais c'est vrai. Tout est attaqué et les bureaux d'enregistrement et les registres ne sont pas l'exception ; pas du tout. Ce n'est pas qu'ils ne vont pas être attaqués parce qu'ils envoient des conséquences de ce problème. Le Google data ID par exemple. Ils venaient de mentionner ma crainte principale ; est ce qu'on peut faire quelque chose? Est ce qu'on peut faire des attaques. Est ce qu'on peut aller dire qu'on va modifier un enregistrement et en même temps on pourrait ne pas le faire. On pourrait décider, avec une logique, de faire une sélection si on va entrer dans les registres et les bureaux d'enregistrement, d'aller faire les enregistrements pour les bureaux et que le reste des gens doivent le résoudre eux-mêmes. Si c'est… qui attaquent tout le monde ou alors même les attaques de hameçonnage.

Je pense que cette transition est faite à partir d'un dénie de service pas intelligent jusqu'à l'attaque envers les registres et les bureaux d'enregistrement. Mais je pense qu'il va y avoir ce genre d'attaques avec des capacités augmentées aussi.

BRAD WHITE: Vous avez une deuxième question monsieur?

JEFF BRUEGGEMAN: C'est un problème très connu ; lors de notre plan de traitement de renforcement de capacité, on a essayé de les aider à développer des procédures et des solutions de technologie. Je n'étais pas présent lors de cette réunion ; mais j'aurais bien apprécié ton commentaire Dan. Et c'est un problème qui est très bien connu ; je ne sais pas si on a une réponse cohérente du secteur de l'industrie

PAUL TWOMEY: Si on attaque des centaines de personnes, on ne peut pas aller dire bon l'ICANN ne fait pas ceci, ne fait pas cela ; mais on doit montrer ce qu'on fait. Mais en tout début, on doit définir ce que l'ICANN est. Et je sais combien de personnes ont contribué à la création d'une institution, une organisation qui travaille sur des aspects exécutifs, qui cherche à financer des activités. Faut pas oublier que dans les années 90 on parlait de la formation d'une communauté qui devait avoir des parties prenantes qui se réunissaient et s'engageaient e je pense que c'est un sujet classique lorsqu'on a une interaction de personnes et qu'on essaye de clarifier ce que les gens espèrent de nous, ce qu'ils attendent de

nous, ce qu'ils espèrent voir. Si on leurs montre ce qu'on fait et ce qu'on ne fait pas, on doit leurs expliquer qui c'est qui opère les zones racines ; les gouvernements sentent qu'ils doivent parler avec eux directement et Mickey est venu précisément parler de cela. On n'a pas beaucoup de gens qui viennent du secteur gouvernemental en ce moment, ici dans cette salle ; mais ce qui me préoccupe, je pense aux crises. Je pense bien sûr que ces crises vont avoir lieu et qu'on devrait faire parler les regroupements et qu'ils nous disent quelle est l'approche commune, quel est leur point de vue commun sur la transparence et les processus. Si on se… aujourd'hui et on se dit bon Patric va faire ça et ça, on s'est trompé. Mais on a besoin d'avoir une participation des gens parce que ce qui est important est que notre projet est multipartite ; c'est un modèle multipartite. Parce que comme Alejandra disait lorsque ces attaques commencent à circuler, on devrait trouver la façon de dire, on est tous d'accord sur ces points, vous avez tous été d'accord lorsqu'on les a signé. Parce que tout le monde aura un plan B…. tout le monde a un plan B et si on me dit que la solution est inutile, on va trouver un plan B bien sûr. Il faut qu'on travaille ensemble dessus. Et on parlait d'une attaque sur internet qui aurait un impact sur les Etats-Unis par exemple comme c'était le 11-09. Apres le 11-09, la communauté américaine a payé un billion de dollars pour faire la guerre. Donc, ce genre de mesure peut provoquer des impacts énormes et on doit considérer que les parties prenantes doivent discuter quel est leur but commun et non seulement.

BRAD WHITE: Debbie?

DEBBIE MONOHAN: J'ai dit tout à l'heure, qu'on devait avoir un rôle de coordination à l'ICANN et que les ccTLD avaient beaucoup à contribuer. Les registres des ccTLD ont beaucoup contribué en terme d'argent à travailler sur ce système et beaucoup ont mis en œuvre des politiques de sécurité pour essayer de minimiser les risques de système de bureau d'enregistrement et on a trouvé une politique de sécurité, on essayé de faire au moins et les bureaux d'enregistrement à travers ce système sont le fond de l'équipe. Parce qu'entre les registres et les bureaux d'enregistrement, ils doivent s'assurer qu'il n'y ait pas de problème de vulnérabilité. On a essayé de les mettre au front en premier lieu pour mitiger ces risques donc je pense qu'on a contribué avec ce qu'on a ouvert et on doit parler à la communauté ICANN. Toutes les parties prenantes doivent contribuer aussi parce que personne n'a la bonne réponse ; on doit contribuer pour écrire ensemble les bonnes réponses avec.uk,.nz ou quoi que ce soit pour trouver la bonne solution comme je le disais. Le rôle de l'ICANN est de coordonner cet échange d'informations.

BRAD WHITE: Paul, je voudrais reprendre ce que tu as dit ; tu as dit qu'on n'a pas assez de gens du secteur gouvernemental dans cette salle et tu voyages avec des fonctionnaires tout le temps. Ils sont… les fonctionnaires pensent aux institutions, ils ne sont pas proactifs ; comment est ce que tu penses que cet aspect impactera sur leur engagement lorsqu'ils viendront?

PAUL TWOMEY: Merci, je pense qu'on a un grand dialogue entre les gouvernements sur la cyber-sécurité en ce moment, ils pensent à servir la cyber-sécurité et ce qu'ils ont fait était de trouver la couche du milieu qui fonctionne de façon différente et de faire attention à ce fait. Mais, ils ne peuvent pas se baser sur le fait qu'on ait une seule génération de personnes qui travaillent toujours sur le système. Il faut qu'il y'ait et que la communauté doit faire partie non seulement de ce groupe mais que les parties prenantes doivent avoir une voie où elles diront on doit aider les gens et avoir une voie dans chaque pays. Je pense que les gens ont dit sur la capacité de plateforme d'informations de la communauté.

CATH GOULDING: Bonjour. Je suis Cath Goulding de Nominet. Je suis une nouvelle arrivante dans cet entourage mais je connais bien les cyber-menaces et je m'excuse si ma question est un peu trop simple ; mais on voit des registres nationaux qui peuvent être menacés par du terrorisme, même un volcan en éruption en Scandinavie et les gens qui sont déconnectés. Donc on a des problèmes massifs dans les registres et on a aussi des stratégies de sécurité qui ont commencé à travailler, à agir sur ces problèmes. Ma question porte sur l'ICANN et les DNS de la racine. C'est qu'on n'a pas une menace internationale, on n'a pas un registre international mais je voudrais savoir si on a un registre de risque pour la racine DNS et si ce ne serait pas une bonne mesure de créer ce registre de risques pour le DNS racine.

BRAD WHITE: Steve, tu échappes à la question?

STEVE CROCKER: Non, je m'excuse mais j'ai une autre séance.

JEFF BRUEGGEMAN: Bon anniversaire, Steve.

STEVE CROCKER: Merci.

BRAD WHITE: Le Dr. Crocker a 17 ans aujourd'hui.

JEFF BRUEGGEMAN: On a des exercices sur la racine et on a des jeux même sur des plans de contingence et on voit beaucoup d'activité autour de la racine ; mais rappelles toi ce ne sont pas les opérateurs de la racine, c'est simplement les NTIA, VeriSign et les racines d'ICANN. Ce que les opérateurs de racine individuels font c'est ce que les racines individuelles font. Donc, lorsque tu as vu comment un agit, tu les as tous vu.

JEFF MOSS: Du point de vue de quelqu'un qui travaille contre ces aspects, la racine est merveilleuse mais elle est trop grande.

JEFF BRUEGGEMAN: Trop grande comment?

JEFF MOSS: La racine n'est pas… c'est-à-dire lorsque je pense que quelqu'un m'a attaqué le DNS, je ne pense pas à la racine ; d'abord parce qu'on a des racines qui sont très bien stockée et on en a pas autant parce que le cacher, quand c'est caché, ce n'est pas toutes les requêtes qui passent par la zone racine. Ce que je veux dire, et je veux que m'entendiez tous, que vous m'écoutiez, lorsque je me préoccupe par rapport aux attaques qui vont impacter sur le DNS, la racine est une belle cible mais ce n'est pas la cible primordiale. Les principales cibles sont les serveurs de noms pour les organisations individuelles sur lesquelles on veut avoir un impact ou alors les bureaux d'enregistrement et les registres qui soutiennent ces registres, ces enregistrements. C'est-à-dire qu'ils envoient ces archives à d'autres registres ; c'est là que vous avez moins d'attention qui est plus exposé. Si vous pensez aux services du serveur racine et si on les expose, on expose les DNS de racine et c'est tout. Aujourd'hui les serveurs de noms de domaine sont plus des hôtes que les DNS ; on a la sécurité web et ce pourrait être un échec de la sécurité internet si on les attaques. Voila mon point de vue.

AMY MUSHAHWAR: Bonjour. Mon nom est Amy Mushahwar, je suis avec Reed Smith et je représente l'association de publicistes du canada. On n'a pas vu de politique de sécurité à travers la publicité mais mon groupe représente un grand nombre de marques internationales et des Etats-Unis parce que mon association est basée au Etats-Unis et pas au canada. Mais alors ; en terme de sécurité, ce qui me préoccupe n'est pas le statut de l'infrastructure ni la possibilité de comprendre ce qui se passe avec une attaque ou lorsqu'on a reçu une menace. Ce qui me préoccupe est le ROI en terme de d'utilisation du DNS en soi-même et si on pouvait se

servir des protections qu'on a avec la protection des marques déposées et des noms faux sans avoir commis d'infraction. Donc l'équipe de sécurité devrait travailler avec l'IPC et développer des protections pour les gTLD parce que bien sûr on est toujours préoccupé par les attaques mais on pourrait avoir un ROI qui est indépendant des attaques et on doit aussi le considérer.

BRAD WHITE: On me dit qu'on doit s'arrêter, apparemment on n'a plus de temps ; ce qui est intéressant il me parait est que tout le monde est venu parler de l'importance de la participation des parties prenantes et comment on doit continuer à les faire participer. Peut être ce panel peut venir à la prochaine réunion et continuer de travailler avec eux.

JEFF BRUEGGEMAN: Combien parmi vous ont cru que ce panel était intéressant? Est ce que vous croyez qu'on doit continuer à le faire dans toutes les réunions? Alors j'espère que vous aurez des questions la prochaine fois. Je voulais dire que beaucoup parmi nous sont venus pour toute la conférence et vous pouvez venir me voir si vous voulez me parler en privée ou à l'équipe de sécurité. Donc merci d'être venu.

BRAD WHITE: Vous avez été merveilleux, on vous remercie de tout cœur.

FIN DE LA TRANSCRIPTION.