TIJANI BEN JEMAA: Merci, Bonjour, bonsoir à tous. Aujourd'hui, nous avons notre sixième webinaire. Donc, notre programme de formation de compétences d'At-Large et d'ALAC. Pour les représentants des ALS, aujourd'hui nous avons Julie Hammer qui va nous parler de la sécurité et de la stabilité du DNS. Elle a une présentation qu'elle va nous faire sur Adobe Connect et je vais d'abord donner la parole à Terri pour qu'elle nous explique un petit peu comment nous allons travailler. Bien Terri, vous avez la parole.

TERRI AGNEW: Merci Tijani. Bonjour à tous, bonsoir à tous, bienvenue à ce webinaire PRE-ATALS II sur la sécurité et la stabilité du DNS, jeudi 15 mai, 15 heures UTC. Nous allons maintenant commencer l'appel. S'il vous plait, je vais demander à tous ceux qui participent de mettre leurs ordinateurs en muet et de donner votre nom lorsque vous prenez la parole pour permettre aux interprètes de vous identifier sur le canal et pour la transcription. Nous avons une interprétation en français et en espagnol. Merci beaucoup Tijani, vous avez la parole.

TIJANI BEN JEMAA: Julie Hammer est prête pour nous faire cette présentation.

JULIE HAMMER: Bonjour à vous.

TIJANI BEN JEMAA: Et nous vous donnons la parole Julie.

JULIE HAMMER: Bonjour, merci Tijani. Bonjour, bonsoir à tout le monde. Bien, donc, je vais commencer et à vous fournir quelques informations sur le rôle d'ICANN dans le domaine de la sécurité et la stabilité du DNS et ce webinaire va définir la sécurité et la stabilité, premier point. Le deuxième point, définir le rôle d'ICANN dans ce domaine là. Ensuite, je vais vous expliquer pourquoi la sécurité et la stabilité sont importantes. Ensuite, nous allons parler de la sécurité, de la stabilité et du comité consultatif dans ce domaine: le SSAC. Ensuite, je vais vous donner un exemple d'une attaque contre la sécurité de l'internet et ensuite nous passons au [inaudible 00:2 ; 17].

Ensuite, il y a aussi l'aspect technique qui vise à préserver, à renforcer la sécurité et la stabilité et la résilience de ce système. Et ce système qui a assigne donc, le système d'identificateur unique de l'internet. Donc, il y a une mission pour coordonner l'assignation des systèmes d'identificateurs d'internet. Ensuite, notre mission pour maintenir et opérer le serveur de nom de la zone racine comme supervision de la communauté et ensuite la gestion des systèmes internes d'ICANN et la fourniture d'un système accessible pour le public afin de diffuser les informations et c'est une mission en même temps technique et autre.

Quel sont les définitions maintenant de la sécurité, de la stabilité et de la résilience?

D'abord la sécurité, il s'agit de la capacité à protéger et à prévenir une mauvaise utilisation des identificateurs uniques de l'internet et bien sûr lorsque je parle de cela, je parle du système de noms et de nombres de l'internet. La définition et la stabilité maintenant, il s'agit de la capacité à assurer que le système opère comme on attend à ce qu'ils le fassent et que les utilisateurs des identificateurs uniques ont confiance que ce système va opérer et fonctionner correctement.

Et la définition de la résilience, il s'agit de la capacité du système d'identificateur unique à tolérer, soutenir et à survivre à des attaques malveillantes et à d'autres problèmes d'interruption et sans que cela donne lieu justement à une cessation ou à une interruption du système de services de l'internet, voila.

Maintenant, il faut souligner que le rôle d'ICANN comprend une série de choses et d'autres choses qui ne correspondent pas au rôle d'ICANN et je pense que c'est important de savoir ce qu'ICANN n'est pas. Pour mieux comprendre ce qu'est l'ICANN dans ce contexte de sécurité et de stabilité. D'abord, ICANN n'est pas une agence de respect de la loi, ce n'est pas un tribunal, ce n'est pas une agence gouvernementale non plus. Donc, l'application de la loi, le respect de la loi et les gouvernements participent comme parties prenantes dans le processus d'ICANN et dans le développement des politiques. Mais ICANN lui-même ne travaille pas dans le domaine de l'application. Donc, ICANN n'est pas responsable pour la politique sur l'internet ou le combat contre des comportements délictueux.

ICANN n'est pas responsable de l'interdiction de sites, des conduites illicites sur l'internet. ICANN n'est pas la partie responsable de tout ce

qui le cyber espionnage et le cyber guerre sur internet. Et ICANN n'est pas autorisé à suspendre de manière unilatérale ou à annuler un nom de domaine.

Maintenant que j'ai expliqué cela, ICANN est capable [inaudible 00:05:43]. Alors, que fait ICANN? ICANN joue un rôle pour soutenir le travail des services d'application de respect de la loi ou le gouvernement des agences gouvernementales pour mettre en place ces actions légitimes à leurs demandes et nous devons voir ici le cadre légal particulier, le contexte particulier dans lequel ICANN fonctionne.

ICANN participe dans le domaine ou avec la communié de sécurité opérationnelle pour étudier, analyser et identifier les usages malhonnêtes ou l'abus du DNS et ICANN joue le même rôle que toutes les parties prenantes intéressées en ce qui concerne les protocoles de l'internet. Et actuellement, l'évolution des protocoles de l'internet et des standards liés à l'internet ne sont pas dans les limites de l'ICANN, mais sont sous la responsabilité du groupe de travail d'ingénierie de l'internet et du conseil d'architecture de l'internet, IETF et IAB sont les sigles qui correspondent donc à ces agences, à ces organismes.

Maintenant que nous donc défini cela, comment fonctionne la sécurité, la stabilité et la résilience au sein d'ICANN? Comment ce rôle se manifeste-t-il?

D'abord, quand on parle de sécurité au niveau d'ICANN, une des valeurs principales qui existent au sein d'ICANN en accord avec l'affirmation des engagements de l'ICANN et avec le département du commerce des Etats-Unis. Ensuite, la sécurité est une des quatre secteurs de

focalisation du plan stratégique de l'ICANN. La sécurité est vraiment un thème général qui appartient à pratiquement toute l'organisation au sein d'ICANN et au niveau organisationnel, il y a un département au sein d'ICANN. ICANN a une équipe qui se consacre à la question de la sécurité qui analyse les problèmes de sécurité et qui travaille dans ce domaine au sein d'ICANN.

La sécurité est un élément essentiel dans tous les projets, dans toutes les activités mises en place par ICANN et finalement, la sécurité est un groupe de parties prenantes clé au sein de la communauté d'ICANN. Il s'agit du comité consultatif de sécurité et de stabilité qui s'appelle le SSAC.

Maintenant voyons pourquoi est ce que la sécurité et la stabilité sont ainsi importantes au sein d'ICANN. Je pense que c'est clair pour tout le monde, mais de toute façon, nous allons essayer de le définir dans les termes plus spécifiques et les points principaux seraient de c'est que la sécurité et la stabilité du nom du système de noms de domaines au sein d'ICANN, la sécurité et la stabilité contribuent à la stabilité de l'environnement économique mondial et il permet une prospérité pour les pays en développement et les pays développés.

L'internet et le système de noms de domaines aide ces nations à mettre en place son réseau. Il soutient la sécurité nationale et l'application de la loi et de l'ordre en général. La sécurité et la stabilité permet un fonctionnement correct de l'infrastructure critique du monde entier. Cela renforce les opportunités pour les commerce en général et cela permet un flux libre de l'information et de la circulation libre de

l'information et cela protège les intérêts des utilisateurs individuels de l'internet.

Par conséquent, vous voyez que c'est très important pour les échanges entre les individus pour que ces échanges et le cadre fonctionne au niveau mondial et il faut tenir de tous ces aspects.

Maintenant, je voudrai vous donner quelques informations sur le comité consultatif de stabilité et de sécurité qui s'appelle le SSAC qui conseille la communauté d'ICANN et son rôle est de conseiller la communauté de l'ICANN et le conseil d'administration de l'ICANN sur des questions qui concernent la sécurité et l'intégrité du système d'assignation d'adresses et de noms de l'internet. Le SSAC a été fondé en 2001, il a commencé à opérer en 2002 et il a commencé à offrir ces conseils au conseil d'administration d'ICANN. Il a soutenu le comité consultatif d'organisation et le personnel et la communauté en général. Et tous les membres sont nommés par ICANN pour trois ans.

Maintenant, les activités du SSAC. Elles sont nombreuses. Ils ont des activités au niveau interne. Donc, d'abord, on a un comité avec des membres qui forment le SSAC, les membres entrent dans le SSAC pour trois ans. Donc, ils rentrent après un entretien et avec le comité de nomination. ICANN fait beaucoup de travail pour présenter des ateliers sur le DNSSEC et des réunions avec les responsables du respect de la loi et le secteur de la sensibilisation des réunions avec le SSAC pour présenter différents aspects de la question.

Il y a aussi un atelier annuel du SSAC qui réunit les différentes parties prenantes et qui fait des révisions du plan de travail etc. ensuite, le SSAC

a aussi différentes parties qui travaillent pour aborder les aspects critiques. Par exemple, les parties de ce groupe de travail analysent les systèmes des paramètres et les abus d'identificateurs, les lignes des sites publics. On travaille aussi sur la contribution à donner pour la transition de fonction IANA et on regarde actuellement la possibilité d'apporter aussi des commentaires, des contributions sur les commentaires concernant le rapport du JAS.

Et maintenant, rapidement, je vais vous donner une petite idée du système de publication qui a été fait par SSAC au cours de cette dernière année. Ce sont des rapports sur la sécurité du DNS qui ont été publiés et à travers le une liste de processus. On a eu un rapport sur la mitigation du risque collision de noms. On a eu une lettre au conseil de l'ICANN concernant l'étude interdisciplinaire. On a eu aussi un rapport, un conseil sur les certificats des noms internes. Et en ce qui concerne les catégories de ces publications pour l'abus de DNS, on a eu des rapports présentés en 2014 sur les attaques de déni de services distribués contre la structure du DNS et à propos du nom de domaine internationalisé.

Des rapports aussi sur l'enregistrement des données, le système de Whois aussi. Donc, ce que je voudrai maintenant, comme je vous l'ai dit, plutôt qu'essayer de parler de tous les domaines concernant les dénis de services distribués dans le domaine de l'attaque contre la sécurité, je vais vous donner quelques exemples d'attaques. Le premier est ce qu'on appelle un DDOF, c'est-à-dire déni de service. Quelque chose sur laquelle je voudrai vous donner quelque donnée de plus, quelques renseignements de plus. Je suis sûr qu'en cas de déni de service, vous savez que cela rend la machine ou le réseau complètement inutilisable pour les utilisateurs. Et l'attaque du déni de service distribué peut être

lancée par une personne ou une machine, c'est important de le noter aussi.

Donc, ce déni de service distribué utilise donc la réflexion du DNS et l'amplification du DNS pour réaliser une attaque de taux de bits de données qui ont été rapportés comme dépassant 300 gigaoctet par seconde. Il y a des diagrammes qui illustrent cela. L'attaque essaye de bloquer le réseau, les demandes et les réponses sur le réseau et de cette façon, l'émetteur est la cible et ne fonctionne plus et en dessous de cela, il y a une multitude d'attaques et il y a en général différentes attaques comme le spouting ou d'autres thèmes.

L'agresseur génère et transmet des données et essaye de se faire passer pour l'adresse IP et il utilise des protocoles de réponse de demandes pour refléter ou amplifier les réponses et parvenir à une attaque et les données d'attaque dépassent la capacité du réseau. Ce qui fait que la victime n'a plus la possibilité d'opérer et il y a bien sûr d'autres attaques contre le DNS.

Le DNS qui va opérer selon un protocole de demandes et de réponses est vulnérable pour ce type d'attaques. Par conséquent, je vais vous donner maintenant quelques explications concernant ce type d'attaques. On a un réseau qui est prévu avec une autorité, un serveur de noms autorité qui est un serveur de noms qui donne des réponses en réponse à des questions posées sur des noms dans des zones données.

Donc, si quelqu'un essaye de signer un nom de domaine particulier ou un site internet particulier, cela va envoyer une demande au serveur de noms autorisé et ce serveur de nom va répondre avec l'adresse du nom

de domaine et le serveur de nom autorisé est par définition ce qui va donner le nom. Un serveur de nom récursif ou serveur de noms de cache est un serveur qui va stocker des résultats des demandes du DNS dans une certaine période de temps et donc, c'est un serveur qui va être mis en place par des organisations pour essayer de gagner du temps en rendant les choses plus rapides quand on a cette demande et c'est un serveur qui ne possède pas la réponse à une demande, va demander à un serveur de noms faisant autorité.

Un serveur de noms récursif peut être sécurisé. Il va répondre seulement aux demandes de sources autorisées dans les réseau ou bien c'est une très bonne façon de concevoir ce type de serveur de noms récursif, par exemple pour une organisation particulière qui va mettre en place un serveur de noms récursif qui va le sécuriser en lui permettant de ne répondre qu'à certaines demandes de noms de machines ou de réseaux autorisés. Ensuite, ce serveur de noms récursifs peut être ouvert et il va répondre à toutes les demandes peu importe la source de ces demandes et c'est souvent le problème justement qui donne lieu aux attaques de déni de services distribués.

On voit maintenant le schéma et vous voyez, le coordinateur de la victime et en dessous et en dessus vous avez la personne qui l'attaque. On a un exemple où la personne qui attaque va se faire le serveur de DNS ouvert et simule, en fait, être la victime. Donc, elle va utiliser l'adresse IP de la victime et va envoyer des requêtes au serveur au résolveur pour lui demander où un nom de domaine se trouve. Alors, le résolveur va remettre cette requête à une quantité de serveurs de noms de domaines faisant autorité et va obtenir des réponses pour ces requêtes, mais la réponse ne vient pas à la personne qui fait l'attaque

bien sûr. La personne faisait semblant d'avoir l'adresse IP de la victime alors, c'est la victime qui va recevoir la réponse et plus de requêtes que la personne faisant l'attaque va envoyer, plus de réponses la victime va recevoir.

Maintenant, pour le cas de droite, on montre une attaque qui déclenche un BotNet.il contrôle un Botnet. Il va envoyer une seule requête et c'est le bot net qui va envoyer ou renvoyer la même requête à plusieurs constamment. Donc, les serveurs de noms de domaines faisant autorité vont envoyer toutes les réponses constamment à la victime. Donc, c'est la victime qui reçoit toujours les réponses ce qui excède la capacité de son réseau.

Alors, les facteurs qui contribuent à cette attaque. Donc les contrôles de base essentiels pour l'accès au réseau et la sécurité du DNS n'ont pas été mis en œuvre dans le mesure du nécessaire pour pouvoir entretenir et élargir un réseau internent résilient. Donc, le serveur de noms de domaines moins de dix ne sont pas suffisamment sécurisé et n'arrivent pas à répondre uniquement aux requêtes venant des utilisateurs autorisés. D'autre part, il y a aussi à chaque fois plus de connexion internet de haut débit et donc, on a à chaque fois plus de dispositifs connectés, ce qui veut dire qu'on a une capacité de plus en plus grande et une quantité d'utilisateurs et de dispositifs de plus en plus larges aussi sur l'ICANN.

On devra prendre des mesures de sécurité pour prévenir les attaques pour les éviter. Alors, plus on a de capacités de débits sur internet, le plus ces attaquants ont la possibilité de nous atteindre. Alors, SSAC a proposé des recommandations, le rapport SSAC 065 à la suite des

considérations de ces questions sans que l'ICANN n'aurait céder à faciliter des efforts et des initiatives de toute la communauté d'internet pour aider à réduire la quantité de réseaux et de résolveurs ouverts qui permettent cette imitation des dispositifs des victimes. Cette initiative devait alors essayer de mesurer la fréquence dans laquelle ces résolveurs sont attaqués et sensibiliser les personnes qui font cette initiative et les personnes qui gèrent les serveurs pour les sécuriser.

Alors, ils devaient aider à identifier et à faire la publicité de l'importance du problème, à sensibiliser les gens et expliquer en même temps la nécessité de sécuriser les réseaux pour aider pour aider les opérateurs de réseaux.

En deuxième lieu, tous les opérateurs de réseaux devraient prendre des mesures immédiates pour éviter la congestion des réseaux contre le spouting des adresses des réseaux et cela peut être fait en vérifiant si les requêtes reçus viennent vraiment d'un utilisateur d'où elles viennent et si les identités sont vérifiées, ils peuvent répondre ou comment ils répondent. C'est ce qu'on appelle le filtre de réception des réseaux.

En troisième lieu, les opérateurs des serveurs DNS récursifs devaient prendre des mesures immédiates pour sécuriser les serveurs DNS récursifs ouverts et ils doivent être capables de ne répondre qu'aux requêtes qui viennent des sources autorisées du réseau.

En quatrième lieu, les opérateurs de serveurs DNS faisant autorité et les serveurs de noms qui doivent absolument répondre à toutes les requêtes devraient soutenir la justification autoritaire d'une limite pour les taux de réponses. Il y a des vendeurs des serveurs qui ont limité la

quantité de réponses qui doivent être transmises à une quantité limité dans une période de temps spécifique et donc à travers cela, lorsqu'il y a une attaque de Ddos, si la quantité de requêtes dépasse une quantité spécifique, l'autorité du serveur ne répondra pas à toutes les requêtes.

Alors, la capacité du réseau ne saura pas dépassée. En cinquième lieu, les opérateurs de serveurs DNS devraient mettre en place les processus opérationnels pour garantir que leurs logiciels de DNS sont mis à jour de façon régulière et pour garantir qu'ils vont communiquer avec leurs vendeurs de logiciels pour être toujours en pas en avant du développement. Il y a toujours de nouvelles vérifications qui surgissent de nouveaux contrôles et si vous réussissez à maintenir votre logiciel à jour, vous allez pouvoir limiter ces attaques.

Autrement, vous n'allez pas pouvoir revenir sur ce qui c'est passé. Le logiciel devrait être capable d'être mis à jour pour prévenir les attaques. Et finalement, les fabricants qui configurent les réseaux des clients devraient utiliser une terminologie spécifique que les organisations et par exemple, les sociétés font cela pour maintenir la ligne des systèmes d'ordinateurs et de réseaux. Donc, ces fabricants devraient prendre des mesures pour sécuriser les dispositifs qu'ils fabriquent et pour garantir qu'ils vont pouvoir les mettre à jour lorsqu'ils seront en utilisation et donc disponibles et ouverts aux attaques parce qu'ils seront vulnérables. Donc, en définitif, ce qu'on veut dire c'est que tout devrait être couvert et mis à jour.

On ne répond pas à des réponses non autorisées. Donc, pour prévenir les attaques ce serait la manière d'avancer et garantir que les dispositifs sont mis à jour, autrement les remplacer. C'est une question de sécurité

bien sûr il y a différentes questions concernant la sécurité qui vont surgir de temps à autre. Mais l'idée de renforcer le rôle de l'ICANN pour maintenir la stabilité et la sécurité du système d'identifiant unique et le système de noms de domaines. C'est l'une des fonctions les plus importantes. Donc, si on protège ces deux systèmes, on protège tous les utilisateurs de l'internet, et pas uniquement le service internet fourni, mais aussi les sociétés, les gouvernements et mêmes les utilisateurs finaux.

Voila la fin de ma présentation et donc je suis prête de répondre à vos questions s'il y en a.

TIJANI BEN JEMAA: Merci Julie. Maintenant, je passe la parole aux participants pour faire des questions. C'est clair. C'était très clair même.

ALAN GREENBERG: Oui, ce n'est pas une question, c'est un commentaire. Dans une diapo, il y avait une liste. On disait que l'ICANN contrôle mais n'est pas responsable. C'est évident qu'on n'est pas responsable de la résolution, mais nous pensons que les problèmes pourraient être identifiés. Donc, ça aurait facilité la résolution des problèmes en tout cas même si on n'est pas responsable. J'espère que vous serez d'accord.

ALAN GREENBERG: la diapo suivante.

TIJANI BEN JEMAA: Oui, bien sûr. C'est un très bon commentaire.

ALAN GREENBERG: lorsqu'on parlait de cyber délit, de cyber travail et qu'on les mentionnait comme faiblesse. On n'est pas responsable de mesures de résolution, mais on pourrait peut être facilité.

JULIE HAMMER: Merci.

TIJANI BEN JEMAA: Merci Julie, merci Alan. Maintenant Olivier Crépin-Leblond.

OLIVIER CRÉPIN-LEBLOND: Merci Tijani. J'ai une question: comment le SSAC.

TIJANI BEN JEMAA: On ne t'entend pas très bien. Ton son est très faible.

OLIVIER CRÉPIN-LEBLOND: Je suis loin. Ça va mieux là?

TIJANI BEN JEMAA: Oui, un peu mieux.

OLIVIER CRÉPIN-LEBLOND: Merci. Alors la question était comment le SSAC identifie les questions à traiter? La communauté At-Large était préoccupée par rapport à la société du DNS et à comment le SSAC s'occupe de cette question.

JULIE HAMMER: Olivier, la réponse à cette dernière partie est que le SSAC répondra aux déclarations des SO et des AC à leurs questions bien sûr. Si vous avez des questions vous voudrez bien les recevoir, il y a un certain temps qui a été remis aux SSAC, une question spécifique et les membres du SSAC sont occupés de cette question et c'était hiérarchisé dans nos priorités pour les mesures annuelles. Des fois ça arrive qu'on reçoit plusieurs commentaires, des suggestions et on doit établir ces priorités. C'est une combinaison qui porte sur les suggestions.

TIJANI BEN JEMAA: Merci Julie. Carlos veut prendre la parole maintenant. Allez-y Carlos.

CARLOS RAÚL GUTIERREZ: Oui, merci Beaucoup Julie de cette présentation qui était magnifique, j'ai beaucoup apprécie cette présentation, mais est ce que la magnitude des problèmes sur les serveurs pourraient être expliqués? Je voudrai savoir de combien d'attaques on parle, de combien de requêtes auxquels les serveurs répondraient par jour? On parle, si on avait des

chiffres, peut être qu'on pourrait convaincre la communauté des faire des efforts.

JULIE HAMMER: Merci Carlos. Le problème est que nous n'avons pas vraiment une notion claire de la quantité d'attaques à la sécurité. On ne connait pas les attentes. Donc, dans les recommandations du SSAC, on pourrait demander d'avoir des statistiques sur la quantité des serveurs faisant autorité. On a, par exemple, le serveur ouvert pour pouvoir le mesurer. Mais cela dépendrait énormément des technologies d'un serveur particulier.

Alors, c'est une des questions, vous voyez, auxquels on ne peut pas répondre. La difficulté dans les opérations du DNS est qu'il s'agit d'une question sur laquelle il faudrait faire des efforts et dans une certaine mesure, ils n'ont pas un bénéfice direct à partir de cela. S'ils ne sont pas vulnérables à ces attaques du DNS en tout cas, donc ils ne le savent pas nécessairement. Et le problème est forcément de convaincre les gens des problèmes.

TIJANI BEN JEMAA: Merci Julie. Nous avons maintenant Otunte Otueneh, Otunte, vous avez la parole. Vous peut être en muet. On ne vous entend pas. Vous nous entendez? Vous pouvez parler? Si on a un problème particulier, on va passer à Alberto Soto pour l'instant. Donc, on viendra sur Otunte. Alberto, vous avez la parole.

ALBERTO SOTO: Merci Tijani. Je comprends la question technique et il me semble que ce qui devrait être convaincu de la sécurité du DNS ne devrait pas être sensibilisé par l'ICANN, mais plutôt par d'autres parties prenantes, par les gouvernements locaux spécifiquement. C'est eux qui sont responsables de la sécurité dans les systèmes informatiques parce qu'en fait toutes les attaques, toutes les vulnérabilités du système d'information ne viennent pas du DNS, ni du système du Whois alors que les personnes pensent que c'et ainsi.

Les utilisateurs finaux croient que leur vulnérabilité vient de l'engagement de l'ICANN, du travail de l'ICANN et ce n'est pas ainsi. Alors, je ne pense que le modèle multipartite.

DAVID: On entend correctement.

ALBERTO SOTO: Donc, les autres parties devraient être engagées. L'ICANN devrait déléguer cela.

TIJANI BEN JEMAA: Julie?

JULIE HAMMER: Merci Alberto. C'est très bien d'agir comme vous l'avez proposé, mais cela ne correspond pas forcément aux gouvernements. Donc, la juridiction du gouvernement devrait s'occuper du domaine national et

alors que certaines de ces attaques sont internationales. Donc, si les gouvernements pouvaient règlementer ce genre de problèmes, c'est très bien. Mais je ne vois pas très bien comment ils pourraient le faire.

TIJANI BEN JEMAA: Merci Julie. Otunte, est ce que vous pouvez parler maintenant? Si vous ne pouvez pas parler, s'il vous plait, baissez la main sur le chat pour qu'on comprenne votre problème. J'ai une autre question au personnel de l'ICANN, est ce qu'il est sur l'Adobe Connect ou est- il communiqué par téléphone?

JULIE HAMMER: Tijani, permet moi de vous relier ce que Moreen m'a dit. Elle m'a raconté qu'il y avait une question de Sunil sur le chat: comment peut-on devenir membre du SSAC?

Le SSAC va mener un processus d'entretien et les membres du SSAC les moins techniques soit disant vont proposer aux SSAC comme étant des liaisons de l'ALAC et le SSAC a une politique qui établit que les personnes que ce soit des liaisons ou pas doivent être acceptés par le SSAC pour participer comme membre permanents avec le droit de vote. Donc, ils doivent suivre un processus de vote et en fait, ils doivent participer à beaucoup d'activités au sein du SSAC parce qu'ils deviennent de membres par les personnes pourraient être proposés en tant que membre par un autre membre du SSAC parce qu'ils ont identifiés une capacité qui manque au SSAC ou peut être parce qu'ils sont intéressés à rejoindre le comité.

Le SSAC, même, a une politique de ne pas être trop grand, de ne pas avoir trop de membres. En ce moment, on est assez nombreux pour ce qu'est la taille habituelle du SSAC et donc c'est un processus beaucoup plus restreint que pour devenir membre de l'ALAC ou des autres comités consultatifs.

TIJANI BEN JEMAA: Merci Julie. J'ai la question d'Outente qui a été publiée sur le chat. Il dit: dans ma région, il y a des problèmes ou des questions d'utilisation sur internet de carte de crédit qui est banni. Alors, quelle pourrait être la raison? D'autre part, il demande que certains fabricants de dispositifs l'aient accusé de mettre des chips de surveillance dans les dispositifs. Est-ce que le SSAC sait cela?

JULIE HAMMER: Pour ces questions de sécurité générale, par exemple si on ne vous permet d'utiliser des carte de crédit sur internet, en fait, je ne suis pas tout à fait sûr si c'est les banques qui ne permettent pas d'utiliser les cartes de crédit sur internet, mais, en fait, ils visent à protéger les informations des utilisateurs, leurs clients. Et bien sûr, ils pourraient faire cela à travers différents moyens, mais je ne suis pas tout à fait sûr de la raison spécifique. Alors, concernant la deuxième question, je vais en revenir un petit peu sur [inaudible 00:35:14].

Alors vous parlez de l'installation de différentes puces dans les dispositifs. Ce n'est pas vraiment une question de DNS. le SSAC s'occupe des questions de sécurité liées aux systèmes de noms et d'adressage sur

internet et ces puces qui doivent être installées dans les dispositifs représentent bien sûr des préoccupations, mais je ne suis pas sûr que ce soit une question de DNS spécifiquement. Et donc, je ne suis pas sûr que cela corresponde au SSAC. Vous voyez, ce n'est pas lié vraiment au DNS.

TIJANI BEN JEMAA: Merci beaucoup Julie. Je comprends ce que vous dites et je vois très bien qu'il ne s'agit pas de questions de sécurité et de stabilité du DNS, ce sont des questions de sécurité dans un sens plus large et ça n'a rien à voir avec le DNS. J'ai Olivier maintenant.

OLIVIER CRÉPIN-LEBLOND: Merci Tijani. Je veux dire que j'étais en train d'écouter la discussion sur la sécurité et la stabilité du DNS et bien sûr que c'est vrai d'une part que la fiabilité du système des noms de domaine et la capacité d'être dérouté, existe bien sûr la mise en œuvre du DNSSEC qui exige que l'on arrête l'utilisation de ces facteurs, ces informations qui empêchent qu'on reçoive le nom de domaine et qu'on a une véritable attaque. Alors, c'est très bien que l'on ait crée le DNSSEC pour prévenir ce genre d'attaques.

Le DNSSEC va se diriger à protéger la sécurité des fonctions sur internet et bien sûr dans le domaine du DNSSEC il serait spécifiquement une solution et ce serait bien d'avoir des informations qui montrent comment le DNSSEC agit pour protéger le système du DNS et pour assurer la stabilité du système.

TIJANI BEN JEMAA: Julie.

JULIE HAMMER: j'aurai dû mentionner cela et j'ai oublié mais c'était un très bon commentaire.

TIJANI BEN JEMAA: Olivier, essayez de trouver la façon de parler devant le micro parce qu'on vous entend vraiment très mal, très loin. On vous comprend à peine. S'il n'y a pas d'autres questions, je profiterai pour remercier Julie Hammer d'avoir fait cette présentation et d'avoir répondue à nos questions. Je vous remercie tous d'avoir assisté à ce webinaire. N'oubliez pas s'il vous plait de remplir la fiche d'évaluation que vous avez reçue avec l'invitation et ces fiches d'évaluation, comme vous savez, vont être utilisées pour améliorer notre programme de formation de compétences. Je vous remercie tous et au revoir.

JULIE HAMMER: Merci Tijani.

TIJANI BEN JEMAA: Merci à tous, merci au personnel, aux interprètes et à tous les participants du programme. Merci.

JULIE HAMMER: Merci à tout le monde. Au revoir.