ICANN79 | Forum de la communauté – Discussion du GAC sur l'atténuation de l'utilisation malveillante du DNS
Lundi 4 mars 2024 – 4h15 à 5h30 SJU

GULTEN TEPE : Bienvenue à la session du GAC qui va traiter de l'atténuation de l'utilisation malveillante du DNS qui se tient le lundi 4 mars à 20 h 15 UTC. Cette session est enregistrée et régie par les normes de comportement attendu de l'ICANN.

Si les questions sont posées dans le chat dans le bon format, elles seront lues à voix haute. Dites votre nom et si vous parlez une autre langue que l'anglais, dites-le. Parlez à un rythme modéré et clairement afin de permettre une interprétation précise. Par ailleurs, éteignez tous vos dispositifs lorsque vous vous exprimez. Toutes les fonctionnalités sont accessibles dans la barre de Zoom.

Nicolas, tu as la parole.

PRÉSIDENT NICO CABALLERO : Merci Gulten.

C'est un plaisir que d'avoir une telle équipe. Sur il y a Alan, un bon ami, il y a Martina Barbero, Susan Chalmers des États-Unis, Nobu Nishigata du Japon qui nous rejoint en ligne, Laureen Kapin et mon cher Nigel Hickson vice-président du Royaume-Uni. Il y a également Laetitia Castillo de la conformité contractuelle de l'ICANN. Il y aura également Alan Woods de CleanDNS.

Cette session va durer une heure quinze. C'est par ailleurs notre dernière session de la journée avant la réception qui sera organisée par .pr. J'espère que vous pourrez nous rejoindre.

Sans plus attendre, bienvenue. Je vais donner la parole à Monsieur Nobu Nishigata du Japon. Nobu, la parole est à vous.

NOBU NISHIGATA : Merci beaucoup, Monsieur le Président, chers collègues. J'espère que vous avez passé une bonne journée. Je ne vais pas vous dire quelle heure il est ici, mais je peux vous dire que c'est la nuit et que j'ai dû rester éveillé très longtemps. Je veux remercier tous ceux qui m'ont permis de vous rejoindre, notamment les collègues de la CPH. Nous avons également eu de l'aide de la part du GAC. Je veux remercier les orateurs précédents de leur présentation, notamment Jamie.

Hier, nous parlions du plan stratégique du GAC et nous avons constaté que l'utilisation malveillante du DNS était une priorité pour nous. Il faut être conscient de la croissance de ce problème. C'est dommage, mais c'est de plus en plus une menace qui pèse sur la sécurité publique. Aussi, on va d'abord écouter la présentation de Laureen, coprésidente du PSWG, et elle va nous parler de ce qui se produit en la matière aux États-Unis. Puis, nous écouterons la présentation d'Alan pour ce qui est de l'évaluation de l'utilisation malveillante du DNS. On a parlé de ce qui était fait au niveau de la CPH et je pense qu'il y a un collègue qui va nous dire davantage à ce propos. Susan va gérer cette partie du débat et ensuite le GAC parlera de ce qu'il peut faire à l'avenir. Ainsi est venu le moment pour nous de prendre les mesures adéquates pour limiter les

utilisations malveillantes du DNS. C'est Martina qui va modérer cette session. J'aimerais vraiment que les collègues nous disent ce qu'ils ont à nous dire et nous sommes disposés à vous écouter.

Sans plus attendre, je vais donner la parole à Laureen. Laureen, vous avez la parole.

LAUREEN KAPIN : Merci beaucoup Nobu. J'imagine qu'il est très, très tard ou très tôt. Mon nom est Laureen Kapin. Je suis coprésidente du groupe de travail sur la sécurité publique. Je suis ravie de pouvoir porter ma casquette de la commission des échanges commerciaux fédéraux des États-Unis. Je suis directrice adjointe pour la protection internationale des consommateurs.

J'aimerais vous parler de nos statistiques de fraudes de 2023. La FTC est une agence d'application du droit civil. Nous poursuivons au civil les pratiques inéquitables et trompeuses. Nous luttons contre toutes sortes d'escroqueries. Nous avons une superbe base de données qui recueille des plaintes venant de tous les services de représentants des consommateurs privés, des organismes de protection et des contributeurs de données internationaux. Nous avons ce qu'on appelle le réseau des sentinelles pour les consommateurs.

Je ne vous ai pas parlé directement d'utilisation malveillante du DNS. Cela a trait au DNS, mais c'est plutôt un aperçu général du type d'escroqueries que l'on constate aux États-Unis. Certaines de ces escroqueries sont facilitées par l'utilisation malveillante de DNS. À l'écran, vous voyez notre aperçu de l'escroquerie en 2023 : 2,6 millions de signalements d'escroquerie, de fraudes. C'est une statistique sans précédent et pour les sommes perdues, c'est aussi sans précédent, 10 milliards. En 2022, il s'agissait de 9 milliards, il y avait également un million de signalements en moins. Il y a une augmentation considérable.

Nos champs principaux sont les usurpations d'identité qui peuvent donner lieu à de l'hameçonnage et ces usurpations peuvent également se faire au détriment d'agences gouvernementales. Il y a d'autres catégories, notamment des plaintes liées aux achats en ligne, des plaintes liées à des tombolas ou des loteries. Il y a également différentes plaintes liées aux investissements ou aux offres d'emploi aux entreprises. En 2023, 4,6 milliards de dollars ont été perdus en raison de fraude à l'investissement, principalement pour ce qui est des

cryptomonnaies. C'est un secteur nouveau qui n'est pas bien compris par le public, donc cela a augmenté.

J'aimerais également attirer votre attention sur les usurpations d'entreprises. Cela a fortement cru en 2023, 742 millions de dollars de pertes. Notre propre agence est frappée également par de telles usurpations. Il y a quelqu'un dans mon bureau qui souffre souvent d'une usurpation et il a des appels de consommateurs et dans ce cas-là, il doit ensuite rapporter cela et déclarer cela comme plainte. Tout le monde est touché par cela. Tout le monde peut se faire escroquer. Ces criminels sont très bons. Si vous pensez être trop malins, vous vous trompez. Ces criminels excellent.

J'aimerais attirer votre attention sur les méthodes de contact. Le courrier électronique a généré le plus grand nombre de rapports. Cela a trait aux sujets que nous traitons dans le cadre de l'utilisation malveillante du DNS. Les courriels sont souvent les méthodes de communication déployées pour les attaques d'hameçonnage.

Ce sont des chiffres sans précédent. Je le disais, les fraudes à l'investissement augmentent, les usurpations augmentent. Regardez tout cela, 10 milliards, 4,6 milliards rien que pour la fraude à l'investissement, 2,7 millions pour les usurpations. Comment est-ce que les victimes payent ? Virements bancaires et cryptomonnaie ; ce sont les principales méthodes de paiement. Pourquoi ? Une fois qu'on transfère de l'argent ainsi, il est très difficile de revenir en arrière, voire impossible.

L'usurpation est la plus commune. Puis, il y a les autres types d'escroqueries que j'ai déjà mentionnées. Nous avons dit que les courriels étaient la méthode la plus fréquente pour contacter les victimes. Puis, il y a également les appels téléphoniques. Les appels étaient en haut du classement depuis très longtemps mais ils ne le sont plus. Il y avait également les SMS.

Qu'est-ce qui génère le plus de pertes ? Ce sont les réseaux sociaux qui sont la méthode de contact qui génère le plus de pertes. Car souvent, sur les réseaux sociaux, on pense traiter avec quelqu'un que l'on connaît. Je pense à l'usurpation d'identité. Puis, il y a également les pop-ups, les pubs en ligne et les sites Web et les applications qui représentent le troisième poste de pertes.

Je voulais parler d'hameçonnage car c'est un sujet qui et précisément de l'utilisation malveillante de DNS. Nous avons reçu près de 1 000 signalements cette année et 100 ce dernier mois, 2,2 millions ont été escroqués cette dernière année. Ce qui se produit le plus souvent, ce sont des usurpations d'entreprises, mais les usurpations d'agences gouvernementales sont également présentes. Nous avons des supports de sensibilisation. Je sais que je reçois beaucoup de courriels ou de messages tels que « Votre colis de la poste est arrivé, mais il y a quelque chose de problématique. Il faut vraiment que vous nous le rappeliez à tout prix. »

Nous recueillons également des informations de nature internationale, pas simplement des données des États-Unis. Il y a des ressortissants étrangers qui se plaignent d'entreprises américaines ou parfois, ce sont

d'autres individus qui parlent d'entreprises étrangères. On peut voir tout cela sur notre portail en ligne. Voici les principales escroqueries. Elles sont assez similaires à celles que j'ai précédemment exposées.

Ceux d'entre vous qui sont curieux pourront consulter nos données publiques sur le site Web de la FTC, ftc.gov si les méthodes de contact mais également les statistiques vous intéressent. Mais si les catégories d'âge vous captivent également, nous avons également des données en la matière. Par exemple, ce sont les catégories d'âge de 30 à 39 ans et de 60 à 69 ans qui signalent le plus d'escroquerie. Ceux qui perdent le plus, c'est la catégorie 60-60.

Ici, il y a quelques références pour vous. Nous avons des données dans notre site Web. Nous avons un document qui regroupe ces données de l'année 2023 ainsi que des informations que vous pouvez consulter en temps réel. Vous pouvez comparer les trimestres, vous pouvez comparer les pertes, les groupes d'âge et les types de contact. Tout cela figure dans notre site Web et nous serons ravis de répondre à vos questions ou vous donner davantage d'informations si vous le souhaitez. Merci beaucoup.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, Laureen. Nous allons voir tout d'abord s'il y a des questions dans la salle ou en ligne. U a-t-il des questions pour Laureen ? Des commentaires ? Aucune main levée. Excusez-moi, Nobu, le Japon, allez-y s'il vous plaît.

NOBU NISHIGATA : Merci beaucoup, Laureen, pour cette présentation. C'est une question peut-être un peu bête, mais est-ce qu'on pourrait savoir dans quelle mesure la technologie des abus du DNS contribue à provoquer ces pertes que vous avez évoquées ?

LAUREEN KAPIN : Nous ne comptabilisons pas ces dommages en termes de catégorie d'abus. Je peux dire que les données de la FTC nous disent que très souvent, les signalements sont facilités par e-mail et par site Web. Cela a un lien direct avec les abus du DNS, notamment lorsque cela est lié à l'hameçonnage. Je ne peux pas dire qu'il y a un lien exact parce que nous ne mesurons pas ces plaintes en lien avec le dévoiement, l'hameçonnage ou d'autres catégories d'abus de DNS. C'est pourquoi j'ai présenté une diapo où l'on parle de l'hameçonnage pour vous donner un avant-goût de ce qui se passe et de ce que nous pouvons voir en termes d'escroqueries.

PRÉSIDENT NICO CABALLERO : Merci le Japon.

L'Inde s'il vous plaît, vous avez la parole.

INDE : Merci beaucoup, Laureen, pour cette présentation. Je suis T. Santosh.

J'aimerais savoir s'il y a des atteintes aux droits de marque aux États-Unis en matière de noms de domaines.

LAUREEN KAPIN : Je suis sûre que cela est le cas. Je ne peux pas vous donner des statistiques de mémoire, mais bien entendu, cela est lié aux escroqueries et il y a une agence spécifique qui s'occupe de cela. Mais cela, bien sûr, est très en lien avec les escroqueries par usurpation d'identité où il y a une entité qui usurpe l'identité d'une autre pour subtiliser des données. Il y a bien évidemment un lien entre ces éléments.

PRÉSIDENT NICO CABALLERO : Merci l'Inde.

J'ai une question pour vous, Laureen. J'aime beaucoup la manière dont vous avez présenté les informations, les schémas, etc. Je pense que vous devez avoir une équipe formidable d'analyse de données. Combien de personnes avez-vous dans votre équipe ?

LAUREEN KAPIN : Nous avons une équipe fantastique d'analyse de données et nous avons une division particulière qui s'occupe de tout cela. Nous avons entre cinq et 10 personnes qui travaillent à l'analyse de données et ils sont vraiment exceptionnels.

Mais il y a une autre équipe qui prépare nos présentations pour que nous puissions les communiquer de manière facile à comprendre pour le public. Nous avons de la chance d'avoir ces équipes.

PRÉSIDENT NICO CABALLERO : Merci beaucoup. Nous en reparlerons plus tard, c'est sûr. Y a-t-il d'autres questions dans la salle ou en ligne ? Le Rwanda.

RWANDA : Je voulais juste savoir, dans la tranche d'âge entre 60 et 69 ans, quels sont les chiffres liés à cette tranche d'âge ?

LAUREEN KAPIN : Je pense que les gens plus âgés d'habitude ont plus d'argent et s'ils ont plus d'argent, ils sont plus sujets à devenir des victimes. Vous avez la possibilité de perdre davantage d'argent si vous en avez plus. Alors que pour les jeunes, ils peuvent devenir des victimes mais comme ils ont moins d'argent, ils perdent moins d'argent. Alors que chez les gens âgés, parfois, il leur arrive de perdre toutes leurs économies malheureusement.

PRÉSIDENT NICO CABALLERO : Merci le Rwanda pour cette question.

Y a-t-il d'autres questions ? Il n'y en a pas. Je vous redonne la parole, Susan.

SUSAN CHALMERS : Merci beaucoup, Nico.

Je vais repasser la parole à Alan Woods de CleanDNS. On va reparler de la question de l'utilisation malveillante du DNS et de la mesure de ces abus.

ALAN WOODS : Je suis le juriste de CleanDNS qui s'occupe des dommages en ligne. Nous essayons d'analyser cette question de manière plus large et c'est pour cela que nous parlons de dommages de manière générale et non seulement d'abus du DNS. Je suis désolé pour les interprètes, mais je parle très vite.

Merci beaucoup, Laureen, pour la présentation que vous avez faite, parce qu'il est important de savoir que ces amendements en matière d'abus du DNS visent à mesurer de manière plus précise tous ces signalements pour essayer de faire une évaluation plus quantitative et connaître l'impact de ces dommages. C'est un point de départ très important lorsque l'on parle de mesurer l'abus du DNS, en particulier à la lumière des nouveaux amendements, des contrats de registre de bureaux d'enregistrement.

Il faut également essayer de considérer cette question du point de vue de la possibilité d'arrêter ou d'interrompre cette utilisation malveillante du DNS pour éviter que ce type d'actions puisse avoir des conséquences sur les victimes.

Je vais présenter les trois principaux points pour moi et pour CleanDNS en matière d'abus de DNS pour mesurer l'impact de ce type d'utilisation malveillante.

Tout d'abord, c'est le concept de preuve exploitable. De quoi s'agit-il ? Quel est le seuil qui doit être franchi pour pouvoir mettre en place des mesures ? Car vous ne pouvez pas mettre en place des mesures si vous

n'avez pas des preuves qui puissent être exploitables. C'est un aspect très important. Comment allons-nous vérifier que ces preuves sont disponibles ?

La question suivante, c'est l'idée d'une action rapide. À quoi fait-on référence ? Il s'agit d'un point de vue assez subjectif : comment on peut mesurer la rapidité lorsqu'on parle d'une réponse à un abus de DNS ? De notre point de vue, cette rapidité doit être accompagnée du concept d'impact de l'abus sur la victime. Pour être sûr s'il y a un impact important, il faut que cette réponse soit encore plus rapide. Encore une fois, la question est de savoir comment nous pouvons mesurer cette rapidité, car c'est un concept assez subjectif.

Ensuite, le dernier concept, c'est celui de pouvoir arrêter et/ou interrompre ces activités. Quelle serait une mesure appropriée au niveau du DNS ? Faut-il suspendre ? Faut-il agir du côté du client ? Faut-il interrompre la résolution ? Que peut-on faire à partir des informations dont on dispose pour éviter tout dommage vis-à-vis de la victime ? Nous savons tous qu'il y a des mesures qu'un opérateur de registre ou un bureau d'enregistrement ne peuvent pas mettre en place.

Voyons quel est l'état de situation pour comprendre où nous en sommes, pourquoi il y a une nouvelle frontière à mesurer pour nous. Pour pouvoir mesurer l'abus du DNS, tout d'abord, nous nous penchons sur des rapports, des signalements. Nous nous penchons sur les listes de blocage et de réputation et sur ce type de documentation. Mais il faut se rappeler qu'un signalement ne veut pas dire qu'un abus a eu lieu. Il faut mettre en place un certain nombre d'analyses pour vérifier

que ce signalement est vrai et pour vérifier qu'il s'agit d'un signalement exploitable.

Du point de vue technique, on peut voir qu'il y a beaucoup de signalements de domaines qui ne sont pas tous accompagnés de preuves exploitables. Il faut voir quelle est la présentation de ces signalements et à partir de cette analyse, nous essayons de voir quel est le ratio de domaines qui sont utilisés pour des actions malveillantes versus le nombre total de noms de domaine. Or, cela ne nous montre pas quelles sont les actions d'atténuation qui sont mises en œuvre. Cela ne nous indique pas comment l'opérateur de registre ou le bureau d'enregistrement réagit à ce signalement. Ce n'est qu'un signalement et il est important de garder à l'esprit cela. Nous devons mesurer le nombre de signalements, mais également il nous faut savoir quelles ont été les actions mises en œuvre pour atténuer ces abus.

Ensuite, quelles sont les attentes par rapport à l'efficacité de ces amendements en matière d'abus de DNS ? Nous devons nous pencher sur le nombre de signalements qui sont accompagnés de preuves. Voilà les attentes de la communauté. Il faut tenir compte des signalements qui sont exploitables, c'est-à-dire qui sont accompagnées de preuves exploitables.

Je vais vous donner un exemple de ce que nous avons pu voir au sein du CleanDNS. J'aimerais vous montrer les informations issues d'une source en particulier sur une période de six mois. Il y a un an, nous avons mesuré le nombre de signalements reçus et je vous invite à regarder cela plus en détail. Il y a plus de 200 000 signalements d'une seule

source dans une période de six mois, et seulement 9 000 de ces signalements totaux ont pu être traités de manière exploitable. Il y a donc beaucoup de signalements qui ne sont pas accompagnés de preuves. Qu'est-ce que je veux dire par là ? Si vous voulez mesurer la santé d'un nom de domaine sur la base des signalements et que vous ne prenez pas en considération combien de ces signalements sont exploitables, en fin de compte, votre métrique sera faussée. C'est ce que nous essayons de faire : essayer d'obtenir des signalements qui soient exploitables avec des preuves exploitables. C'est sur ces signalements que nous devons nous focaliser pour mettre en place des métriques.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, Alan. Je vais vous arrêter là. Nous avons une question ou plutôt un commentaire de l'Iran. L'Iran allez-y, s'il vous plaît.

IRAN : Si vous me permettez, je devais tout juste allumer mon micro, cela prend un petit peu de temps.

Vous avez dit que sur 200 000 signalements, il n'y en a eu que 9 000 qui étaient exploitables. Quelles sont les informations qu'il nous manque ici ? Comment pouvons-nous sensibiliser le public à ce qu'ils nous fournissent davantage de preuves exploitables ? J'espère que les gens ne vont pas me critiquer pour ce que je vais dire, mais quelles sont les informations qui nous manquent et qui peuvent nous induire à faire des

erreurs ? Que pouvons-nous faire pour recueillir des informations plus précises ?

ALAN WOODS : Merci Kavouss. Tu as raison. Dans ce secteur, nous n'avions pas d'abord utilisé des sources ou des attentes. Nous avons utilisé des éléments qui nous aidaient à agir dans le milieu. Il s'agit en fait de faire de meilleurs signalements et de mieux gérer les attentes qui sont imposées aux bureaux d'enregistrement et aux opérateurs de registre afin que l'on ait de bonnes preuves d'emblée.

Si on reçoit les preuves d'emblée plutôt que l'on doive les chercher, cela permet de limiter l'incidence de tels abus. Il faut de meilleurs signalements, de meilleures évaluations et de meilleures preuves envoyées d'emblée. Oui Kavouss, je suis d'accord, il faut avoir une des meilleures conditions pour les preuves sur tous les plans.

IRAN : J'ai une question de suivi. Pourriez-vous nous donner des critères, des conseils, des lignes directrices ? J'aime bien le terme de preuves exploitables, je l'utilise également au sein de l'UIT. Je pense qu'il faut vraiment réfléchir à la façon dont on peut informer la communauté pour qu'elle sache quelles sont les preuves exploitables à envoyer. Ce n'est pas une erreur, c'est plutôt un manque de sensibilisation. J'espère que vous m'avez bien compris. Que peut-on faire pour mieux informer la communauté et qu'elle puisse nous donner des preuves exploitables ? Merci.

ALAN WOODS : Merci Kavouss. Je ne veux pas défendre CleanDNS ici, ce n'est pas l'objectif de ma présentation, mais ce que nous voulons faire, c'est rendre plus ergonomique le processus de signalement. Je vois [inaudible] et Graeme à l'arrière ici de l'Institut de l'abus du DNS ; CleanDNS fournit le backend pour cela. Il s'agit d'un processus de signalement aisé. Il s'agit également de vous donner les bonnes informations quant à ce qui doit être joint au rapport, même pas le destinataire, car ceci, c'est NetBeacon qui va le faire.

Tous les clients qui utilisent notre flux d'ingestion pour la gestion des situations malveillantes bénéficient d'un parcours d'utilisateur très précis. Par ailleurs, on vous indique également à quel fournisseur il faut envoyer le rapport. Parfois, on peut associer un individu, un domaine, mais peut-être que ce n'est pas le bon endroit où il faut faire le signalement, notamment s'il s'agit d'un grand réseau social. Si la plateforme est abusée, l'opérateur de registre ne pourra que transmettre le signalement.

PRÉSIDENT NICO CABALLERO : Merci Alan. Merci pour ces réponses détaillées. Laissons Alan finir sa présentation, puis l'on prendra davantage de questions à la fin.

ALAN WOODS : Je vais sauter une ou deux planches. Je vous invite à vous pencher sur ces planches et nous avons un petit stand dehors, vous pouvez venir

nous parler et nous comblerons les lacunes. Peut-être que l'on pourrait passer le citoyen à la planche *Time to live.*

Si vous n'avez pas lu le SSAC115, je vous invite à le consulter. J'étais moi-même invité à cette session pendant cette session, l'un des éléments qui a émergé, c'est de faire en sorte que la durée de vie soit adéquate. Plus il y a une réponse rapide au rapport, moins il y a de dégâts.

Nous sommes un peu préoccupés par un aspect. Il faut se pencher sur le volet d'utilisation malveillante systémique. Il y a des noms de domaine et il y a des bureaux d'enregistrement qui ne réagissent pas à ces signalements qui ont une forte incidence. Je ne pense pas qu'il faut se concentrer simplement sur les rapports ou les signalements qui sont faits sur des grands opérateurs de registre ou des bureaux d'enregistrement qui sont réactifs ; il faut se concentrer sur la lutte contre les éléments de notre comité qui ne réagissent pas, qui ont une importance dans la communauté mais qui ne répondent pas suffisamment assez rapidement. Il faut évaluer le quantitatif et pas seulement le qualitatif. Il faut réfléchir aux réactions, il faut réfléchir à la façon dont les opérateurs de registre et les bureaux d'enregistrement agissent. Comment réagissent-ils ? Quel est leur objectif subjectif ? Comment est-ce qu'ils réagissent à ces utilisations malveillantes alors qu'elles se produisent ?

Il y a beaucoup de texte à l'écran. Je vais répondre à la question que j'ai posée au départ. Les preuves exploitables, comment va-t-on les éprouver ? Pour rebondir sur ce qu'a dit Kavouss, il faut créer un

minimum de preuves. Il faut établir des standards en matière de preuves, mais également des standards en matière de signalement afin que les opérateurs puissent bien comprendre. Mais nous voulons également vous donner des sources qui vous permettent de collecter ces preuves. Il faut des sources qui en donnent alors.

Pour l'action prompte, je fais référence également au SSAC115, on dit 96 heures, c'est la disposition, mais lorsqu'il y a une incidence grave sur la victime, cela devrait être plus rapide que 96 heures en fonction de la réponse subjective. Et nous devons pouvoir justifier le temps de réaction, évidemment. Puis, il y a l'interruption ou la disruption. Peut-on demander que les parties contractantes clarifient cela au cas par cas ou alors justifient pourquoi ils ont pris ou non telle ou telle mesure ? C'est un autre élément important. L'opérateur de registre ou le bureau d'enregistrement ne doit pas nécessairement toujours agir, mais il faut toujours se pencher sur ce qu'ils ont fait pour soutenir la victime.

Je ne vais pas parler beaucoup plus longtemps, je vous encourage à venir me parler. Il y a beaucoup de questions auxquelles, je l'espère, nous pourrons apporter une réponse. Il y a plusieurs façons d'évaluer cela, nous avons des approches en la matière. Nous pensons pouvoir aider la communauté à réussir le déploiement de ces amendements liés aux dispositions de l'utilisation malveillante du DNS.

PRÉSIDENT NICO CABALLERO : Merci Alan. Je donne la parole aux participants s'il y a des questions pour CleanDNS. Y a-t-il des commentaires, des questions ? L'Iran.

IRAN : Nico, merci d'avoir envoyé l'ordre du jour et merci de l'organisation du programme. On parle de sujets qui sont absolument essentiels. On parle avec les unités constitutives les plus importantes. Je ne te flatte pas ici, je pense vraiment cela.

Je pense qu'il faut mieux communiquer au sein de notre communauté de représentants gouvernementaux. On ne pourra pas tout évoquer maintenant, mais je pense qu'il faudra réfléchir à d'autres outils.

Nico, toi qui cherches toujours des solutions innovantes, je pense que tu pourrais avoir un document, une sorte de circulaire qui pourrait être diffusée auprès des gouvernements faisant état des points les plus importants à traiter et à faire référence à tout cela dans un point de situation et qui s'inspirerait de tout ce qui a été dit pendant ces quatre à cinq jours. Il faut une meilleure communication au sein du GAC. Il y a l'un ou l'autre gouvernement qui n'est pas nécessairement conscient de tout cela ou qui n'est pas suffisamment sensibilisé. Je laisse cela à ta discrétion. Tu trouveras sans aucun doute la façon de mieux communiquer avec les gouvernements afin de renforcer leur conscience du problème.

Je ne suis pas là pour vous faire des leçons, mais je pense qu'il faut sensibiliser davantage tous les individus. Merci.

PRÉSIDENT NICO CABALLERO : Merci, Kavouss, pour le compliment et pour les suggestions. Kavouss, est-ce que tu as une question pour Alan sur CleanDNS ?

IRAN : Non. J'apprécie vraiment les efforts qui sont faits et je pense que le sujet est bien plus complexe que ce que l'on pensait. Il faut vraiment avoir une compréhension mutuelle de nos problèmes. Désormais, nous comprenons quels sont les problèmes pour les gouvernements, mais il nous faut davantage d'informations et une plus grande sensibilisation. Ce n'est peut-être pas utile pour certains, mais ce sera très utile pour beaucoup d'autres.

PRÉSIDENT NICO CABALLERO : Merci à l'Iran.

J'ai le Japon puis le Royaume-Uni. Nobu.

JAPON : Merci Monsieur le Président. Merci de cette présentation, c'est une présentation très utile.

J'ai une question pour les représentants gouvernementaux. Kavouss l'a évoqué également. Les gouvernements peuvent réfléchir à la promptitude avec laquelle ils peuvent réagir pour interrompre ces utilisations malveillantes. Il y a également les preuves exploitables. J'ai une question à propos des normes. S'agit-il de normes à développer ? Ou s'agit-il de normes qui existent déjà et qui doivent être observées par les gouvernements ?

ALAN WOOD : Il y a des normes qui sont élaborées par des acteurs du secteur et je pense qu'il faut se tourner vers le RYSG qui a déjà élaboré des normes en la matière. Il y a également en collaboration avec le groupe de travail sur la sécurité publique pour ce qui est des réseaux zombie et ce qui est nécessaire en matière de mesures et de standards de preuve pour les réseaux zombies. Puis, il y a également le groupe politique de la juridiction Internet. Évidemment, les parties contractantes sont prêtes à relever le défi et à collaborer avec des personnes qui évoluent au sein du système de noms de domaine afin d'établir des normes raisonnables, des seuils raisonnables et des preuves raisonnables.

Nos clients nous ont dit qu'il y avait la nécessité de se pencher sur tout cela. Nous allons évidemment continuer à nous pencher sur les normes et comment elles s'appliquent à la communauté. Mais également, nous voulons avoir une approche réaliste quant à ce qui peut être accompli au niveau des opérateurs de registre et des bureaux d'enregistrement et bientôt sur le plan de l'hébergement. Merci.

PRÉSIDENT NICO CABALLERO : Merci le Japon. Merci Alan pour la question.

Le Japon, vous souhaitez reprendre la parole ?

JAPON : Merci pour la réponse.

PRÉSIDENT NICO CABALLERO : Le Royaume-Uni, Nigel Hickson.

ROYAUME-UNI : Merci beaucoup Alan pour cette présentation qui contient des observations très intéressantes. Je ne parle pas au nom du GAC, mais je pense que vous devriez venir plus souvent nous voir. Ce n'est pas seulement votre accent irlandais, c'est vraiment très informatif, tout ce que vous avez partagé avec nous. J'ai une question pour ce qui est des enregistrements groupés. Avez-vous des remarques à partager par rapport à cette question des enregistrements groupés pour ce qui est de confirmer la validité de ces enregistrements groupés ?

ALAN WOODS : Merci beaucoup pour cette question. On va ici apporter également un autre concept, celui d'enregistrements à prix bas. Cela a un impact sur l'abus du DNS. Mais pour revenir à ma question principale, si on identifie un certain comportement en matière d'enregistrement à bas prix, on peut se douter que des activités malveillantes puissent avoir lieu. Nous avons pu constater également des types d'abus avec des enregistrements qui étaient très chers même. Ce que je veux dire, c'est qu'il y a de bonnes raisons pour effectuer des enregistrements groupés, parce que parfois, c'est la meilleure façon de faire.

Cependant, s'il y a 100 000 domaines – et c'est dans une des me diapos – qui sont enregistrés mais aucun d'autres n'a été utilisé pour effectuer des activités malveillantes alors qu'il y a un seul domaine qui a été utilisé pendant cinq heures et qui a été utilisé pour des activités d'hameçonnage, où doit-on mettre les ressources ? Nous devons nous attaquer à ce domaine qui a mené des activités malveillantes ou doit-

on vérifier ce qui se passe avec ces 100 000 domaines ? Comment faire pour mesurer l'impact ? Je vous invite à analyser l'impact plutôt que les chiffres absolus.

PRÉSIDENT NICO CABALLERO : L'Indonésie.

INDONÉSIE : Je voudrais savoir, parce que je m'inquiète beaucoup quand je lis les statistiques, il y a des gens de 69 ans qui peuvent perdre toutes leurs économies. Moi, j'approche de cet âge et je ne voudrais pas perdre toutes mes économies. Je voudrais savoir, est-ce qu'il y a une unité qui se penche sur les statistiques ? Est-ce qu'il y a une interaction avec les organisations bancaires ? Est-ce qu'il y a un dialogue pour essayer de trouver des moyens de réduire ce type d'abus ? Parce que par exemple, pour obtenir 100 000 dollars… Tout ce que vous montrez dans votre diapo, comment doit-on agir ? Faut-il parler directement avec la banque ? Comment peut-on faire en sorte que l'on puisse trouver le bon correspondant pour signaler le problème ? Est-ce qu'il y a une discussion qui a lieu entre l'ICANN et les institutions bancaires ? Voilà ma question finalement.

PRÉSIDENT NICO CABALLERO : C'est une question pour Alan ?

INDONÉSIE : Je voulais savoir quelles sont les possibilités entre les réglementations bancaires et les réglementations en matière de technologies qui peuvent être mises en place pour éviter ce type d'abus.

ALAN WOODS : Tout d'abord, l'équipe OCTO de l'ICANN fait un travail remarquable. Nous sommes en contact avec eux. Ils développent, ils créent un nouveau système de statistiques qui se penche notamment sur ce que nous voulons rechercher. Il ne se penche pas uniquement sur les chiffres absolus, mais aussi sur des mesures d'atténuation. Je voulais tout d'abord dire cela. Oui, c'est la réponse.

Chez CleanDNS, nous ne nous fions pas uniquement aux sources qui existent déjà. Nous avons des sources qui peuvent être des banques, des départements gouvernementaux, tous ceux qui peuvent nous fournir des signalements basés sur des preuves, et cela non seulement pour nous, mais aussi pour les opérateurs de registre et les bureaux d'enregistrement afin de réduire au minimum ce type d'abus.

Si nous pouvons obtenir un meilleur signalement de la part des banques, de la part des compagnies téléphoniques, cela pourrait avoir un impact. Donc la réponse est oui ; nous sommes en contact avec eux et j'invite les gouvernements ici présents à partager avec nous tout signalement que vous auriez car ces informations sont très utiles pour nous, pour nos clients et pour les gens qui ne sont pas des clients également.

PRÉSIDENT NICO CABALLERO : Merci de l'Indonésie. Merci Alan.

John, est-ce que vous souhaitez dire quelque chose ? Je viens de voir John Crain de l'équipe OCTO de l'ICANN. L'Indonésie si vous voulez prendre contact avec John, il est là dans la salle.

Maintenant je vais passer la parole à l'Inde.

INDE : Merci Monsieur le Président.

Comme cela a été mentionné par Alan, il y a des normes. L'IETF a créé des standards en matière de DNSSEC, d'IPsec, de BGPsec. Quel est l'état de situation par rapport à la mise en œuvre de ces normes ? Est-ce que l'ICANN peut faire en sorte que ces normes puissent être appliquées pour éviter les abus du DNS ?

Ensuite, le travail fait par CleanDNS concerne les domaines qui sont enregistrés par le biais des opérateurs de registre et des bureaux d'enregistrement. Que se passe-t-il avec des domaines qui sont créés dans le réseau Tor, par exemple dans des réseaux parallèles ? Est-ce qu'il y a des informations par rapport à cela ?

ALAN WOOD : Je pense que les questions sont difficiles aujourd'hui.

Première question par rapport à DNSSEC. Je suis juriste, mais je crois qu'il s'agit d'une discussion très importante, notamment lorsque l'on se penche sur des normes minimales que l'on doit respecter.

Tout d'abord, il faut mettre la barre plus haute et avoir ces discussions par rapport au benchmarking pour générer des meilleures pratiques et des pratiques qui soient acceptables. Je pense que c'est une discussion à avoir, certes. J'invite les membres du SSAC et les gens qui s'y connaissent en DNSSEC à participer à ces discussions. Mais je vous le dis, je suis juriste et je pense tout simplement qu'il y a des discussions à avoir par rapport à ces questions.

Ensuite, pour ce qui est des DGA, mon équipe travaille en ce moment à l'identification des DGA pour travailler main dans main dans la main avec les forces de l'ordre. Nous savons qu'ils peuvent identifier beaucoup de DGA qui ont lieu et nous voudrions donc mieux comprendre comment ils peuvent obtenir ces informations.

Je suggère une fois de plus de lire le document qui a été fait par le groupe des représentants des opérateurs de registre en la matière. Et n'hésitez pas à nous contacter car nous essayons d'aider les opérateurs d'enregistrer et les bureaux d'enregistrement à réagir à ce type de cas d'abus, à faire des signalements.

Nous travaillons également à l'élaboration ou la mise en place d'un portail avec les forces de l'ordre pour qu'ils puissent faire leur signalement directement par le biais de ce portail. Encore une fois, je vous invite à nous contacter. Si vous avez les informations dont nous avons besoin, n'hésitez pas à nous les fournir. Merci beaucoup.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, l'Inde, pour la question. Merci Alan pour cette réponse détaillée.

Nouvelle question de Papouasie-Nouvelle-Guinée. Je veux être sûr que nous avons suffisamment de temps pour la présentation des États-Unis et de la Commission européenne. Allez-y, Russell.

PAPOUASIE-NOUVELLE-GUINÉE : Merci beaucoup Alan, chers collègues. Une remarque et un commentaire.

Notre collègue de la FTC a bien précisé que l'enjeu se joue au niveau de la cybersécurité. Les gouvernements de notre région concentrent leur attention sur les problèmes de la cybersécurité. Il y a des initiatives de renforcement de capacités qui sont en place et je voulais savoir si vous êtes actifs, si vous êtes impliqués dans ce type d'activités, dans ces efforts en matière de cybersécurité.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, Russell. Alan, je vous demande d'être bref.

ALAN WOODS : Je vais dire oui, nous essayons de nous impliquer dans ces activités. Chris Lewis Evans travaille en tant que directeur au sein de CleanDNS. Vous le connaissez tous, n'hésitez pas à entrer en contact avec lui pour que nous puissions participer davantage à ces activités de renforcement des capacités.

PRÉSIDENT NICO CABALLERO : Maintenant, je souhaite donner la parole à Martina de la Commission européenne.

MARTINA BARBERO Je pense que c'est une discussion très intéressante. Pouvons-nous passer à la diapo, s'il vous plaît ?

Les trois présentations étaient excellentes avec la conformité. Alan et Laureen, et cela alimente nos réflexions au GAC pour les évolutions futures notamment.

Ce que vous voyez à l'écran ici, ce sont des points qui ont été extraits des commentaires soumis par le GAC lors de juillet dernier pour les amendements apportés au volet contractuel. Ce sont les zones que le GAC a mis en exergue quant à la réponse de la consultation publique dans les secteurs importants qui sont requis par la communauté pour prêter attention au suivi, aux abus du DNS et de l'importance de reconnaître hors et dans l'ICANN. Puis, il y avait également d'autres idées relatives aux PDP, les processus de déclenchement des réponses politiques et la formation. Ces éléments étaient évoqués par le GAC à l'époque. Je pense que c'est par ailleurs pertinent de parler également de la rapidité de la réponse et des preuves exploitables. Ce sont des sujets brûlants toujours. Ce sont des secteurs pour lesquels nous pouvons œuvrer en communauté.

Ce que nous allons faire, c'est d'avoir un bref débat que nous avons déjà lancé par ailleurs avec Alan et Laureen. L'objectif est de répondre à ces

deux questions. Quand est-ce que le GAC peut s'attendre à un point de situation de la conformité pour ce qui est des progrès réalisés pour les abus DNS ? Je sais qu'il n'y a plus que nous entre ce moment et la réception, donc va tenter d'écouter vos perspectives sur les PDP et notamment ce qui résulte des obligations contractuelles. Alan l'a évoqué également, les amendements, ce volet avait trait à relever les ambitions. Et on a également parlé de benchmarking et de bonnes pratiques.

Quand j'ai fini ma présentation, je voulais simplement savoir s'il y avait des représentants du GAC qui avaient des choses à nous dire à ce stade. Je sais que vous avez déjà dit beaucoup de choses, mais il serait toutefois intéressant de savoir ce que vous en pensez.

PRÉSIDENT NICO CABALLERO : Merci à la Commission européenne. C'était assez bref après avoir écouté Alan pendant autant de temps – je plaisante, évidemment. Je donne la parole aux délégués s'ils ont des questions ou des observations. Y a-t-il des mains levées, des retours, des questions ? Ce ne semble pas être le cas. J'ai la Suisse.

SUISSE : Je suis Jorge Cancio pour la Suisse. Je vais briser la glace. Je vais rebondir sur la première question.

Les amendements entrent en vigueur au mois d'avril. Peut-être que l'on pourrait attendre six mois avant un premier rapport. Puis, ce rapport pourrait également évoluer oui au fil du temps, à mesure que la

communauté contribue, à mesure que l'on recueille davantage de données et de retours. Voici ma première réaction.

Quant à la deuxième question, il faut en parler davantage avec les collègues de la communauté. Évidemment, nous pouvons en parler avec la bilatérale avec le conseil de la GNSO pour savoir ce qu'ils en pensent. Merci.

PRÉSIDENT NICO CABALLERO : Merci à la Suisse.

Avant de donner la parole à Susan, je veux demander s'il y a d'autres réactions. Susan, c'est toi qui voulais réagir.

SUSAN CHALMERS : J'ai simplement levé la main. En effet, j'invite tous les représentants du GAC à alimenter nos débats, notamment pour ce qui est de ces deux questions à l'écran.

Au vu de ce que nous avons entendu et au vu également de ce qu'a dit le département de conformité, notamment à propos de leur rapport mensuel, au vu de tout cela, je pense que six mois comme Jorge l'a dit, c'est un délai raisonnable pour analyser les progrès résultant de ces amendements. C'est tout ce que j'avais à dire.

Un peu plus tôt aujourd'hui – et j'essaie de faire émerger le fil rouge de toutes les conversations que nous avons eues aujourd'hui – Chris Disspain a évoqué pendant le bilatérale avec la CPH qu'il faut suffisamment de temps pour mesurer les progrès résultant des nouveaux amendements afin que l'on puisse réfléchir à nos futurs

efforts. Ces efforts à l'avenir devront évidemment se fonder sur l'analyse des résultats des amendements.

PRÉSIDENT NICO CABALLERO : Merci aux États-Unis.

Y a-t-il d'autres demandes de prise de parole à ce stade ? Le Royaume-Uni.

ROYAUME-UNI : Nigel au micro pour le Royaume-Uni.

En deux mots, cela a été très utile. Notre distinguée collègue des États-Unis a raison, il y a un véritable fil rouge qui parcourt tous nos débats. Ce n'est pas nécessairement que je veux apporter une perspective nationale, mais je veux toutefois rebondir sur ce que Laureen a dit, notamment pour ce qui est des statistiques aux États-Unis. Je pense que si nos propres pays se penchaient sur ces statistiques, ils auraient beaucoup à dire à ce propos. Et je pense que cela peint un tableau un peu sombre de la situation.

Oui, il faut évaluer les conséquences des mesures qui ont été prises, des amendements qui ont été adoptés, mais il faudra également que l'on réfléchisse à une élaboration des politiques sur les réseaux zombies ou l'hameçonnage ou peut-être qu'on pourrait au moins commencer à se creuser les méninges et à réfléchi aux éléments qui devraient attirer notre attention ?

PRÉSIDENT NICO CABALLERO : Merci au Royaume-Uni. Laureen, Martina, on peut passer à la suite ? Très bien. J'ai Michele de Black Knight. Puis j'ai l'Iran, puis la Commission européenne. Michele.

MICHELE NEYLON : C'est intéressant de se tourner vers l'avenir, cela a du sens. Mais je ne sais pas si six mois seront suffisants. Pourquoi ? Ces amendements contractuels ont directement trait aux opérateurs de registre et aux bureaux d'enregistrement. Ils n'ont aucune incidence, ils n'ont pas de lien avec les FAI, les fournisseurs d'hébergement. Ce sont d'autres composantes de l'écosystème. En des termes pratiques, lorsque l'on voit des pratiques numériques néfastes qui impliquent un nom de domaine, si le bureau d'enregistrement n'héberge pas le site Web, le service de messagerie électronique qui donne lieu au problème, la seule option, c'est de retirer complètement le nom de domaine de la Toile, ce qui va faire disparaître tous les autres services associés ou alors vous n'avez pas de bistouri, vous avez une masse.

Je comprends que ces amendements vont donner lieu à davantage d'obligation, mais ce n'est pas une panacée. Cela ne va pas résoudre tous les problèmes d'utilisation malveillante de ces outils en ligne. Il y a des éléments qui sont complètement hors de notre champ d'application. Il y a certaines choses que des gouvernements peuvent faire, que d'autres fournisseurs de l'écosystème peuvent faire. Mais tous les problèmes Internet ne peuvent être résolus par les bureaux d'enregistrement et les opérateurs de registre.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, Michele. Merci d'avoir fait référence à Sledgehammer, masse en français.

J'ai l'Iran désormais.

IRAN : Il faut un point de situation graduel. Six mois, c'est d'abord raisonnable il me semble pour un premier retour. Évidemment, on pourrait revenir par la suite et avoir davantage d'informations.

J'avais autre chose à dire. A-t-on une liste de pays ou d'entités qui ont signalé des utilisations malveillantes ? Sur les 206 pays et territoires, combien ont signalé des utilisations malveillantes ? Un ou deux ou trois pays, ce n'est pas suffisant. Il faut un aperçu complet. S'il y a des pays qui n'ont rien à signaler, que cela signifie-t-il ? Qu'il n'y a pas d'utilisation malveillante, qu'ils ne l'ont pas identifié ou qu'ils ont peut-être un creux ? Je ne sais pas. Je pense qu'il serait bon d'avoir une liste des pays ou du moins un aperçu régional de ces problèmes, quelques pourcentages du moins afin de savoir qui a signalé des utilisations malveillantes. Je sais que de nombreux pays n'ont rien signalé, mais cela ne veut pas nécessairement dire qu'il n'y a pas d'utilisations malveillantes. J'aimerais connaître l'état des lieux, merci.

PRÉSIDENT NICO CABALLERO : Merci à l'Iran pour ces observations.

J'ai la Commission européenne à moins que Laureen souhaite réagir.

LAUREEN KAPIN : Très brièvement, Kavouss souligne un point très important. Les individus savent-ils où signaler les utilisations malveillantes ? Les bureaux d'enregistrement, les fournisseurs d'hébergement, l'ICANN, les autres entités qui jouissent d'une responsabilité ? Je pense que tous les efforts de communication, de sensibilisation de la communauté revêtent une grande importance. On n'a qu'une perspective partielle de l'ICANN. Même dans mon agence, on n'a qu'un aperçu partiel. On sait que tout cela ne fait l'objet d'un signalement que partiel. Il faut sensibiliser, communiquer, dire aux individus où ils peuvent signaler leurs problèmes.

PRÉSIDENT NICO CABALLERO : Merci Laureen.

La Commission européenne désormais.

COMMISSION EUROPÉRENNE : Merci Nico. Gemma Carolillo de la Commission européenne.

Je suis en solidarité totale avec Nobu, c'est le soir ici. Je ne veux pas entre en concurrence avec le Japon à ce propos. Bonjour de Bruxelles. Merci à tous les intervenants, les débats étaient très enrichissants. Il y a eu beaucoup d'informations captivantes qui ont été exposées, notamment en provenance de la conformité de l'ICANN.

J'ai cru comprendre que les rapports seront faits de façon régulière et peut-être à une fréquence plus rapide que six mois. Peut-être que ce peut être mensuel et je pense qu'à mesure que le temps passe, il y aura

de plus en plus de preuves recueillies et que les rapports seront de plus en plus touffus.

Il y a des références dans la présentation de CleanDNS à des sujets pour lesquels le GAC œuvre. J'en arrive à ma deuxième question. Je pense que là où le bât blesse, c'est plutôt au niveau qualitatif que quantitatif. Parfois, il ne faut pas beaucoup de signalements pour avoir des dégâts considérables. Il ne suffit que d'une seule grande campagne d'hameçonnage pour créer des dégâts d'envergure. Ce n'est pas simplement une question du nombre de rapports.

Évidemment, il y a une complexité au niveau des sources qui permettent d'identifier les sources d'utilisation malveillante. L'objectif est d'empêcher tout dommage. En fin de compte, il faut arrêter et ces utilisations malveillantes, il faut prévenir tout dégât.

Je pense qu'il faut que l'on continue à réfléchir aux normes minimales, au benchmarking afin qu'il y ait des informations claires quant à ce que sont les preuves exploitables, comment il est possible de recueillir des preuves exploitables, notamment la façon dont ces preuves exploitables peuvent prévenir tout dommage ou préjudice.

Par ailleurs, je veux répéter que le nombre de signalements n'est pas nécessairement le témoin de la santé d'un domaine ou d'un domaine de premier niveau. Par ailleurs, je pense que l'on peut également améliorer la qualité des signalements. Tout cela est lié à la transparence.

Évidemment, je ne dis rien de nouveau, je dis tout simplement que ces présentations m'ont conforté dans notre position. Le GAC avait déjà des axes de travail qui étaient liés à tous ces éléments qui ont été soumis. Je veux à nouveau remercier le GAC d'avoir organisé un tel débat. Il faut continuer à discuter de cela. Il faut que l'on réfléchisse encore aux normes minimales et à la façon dont on pourra le mettre en place. Merci beaucoup.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, la Commission européenne.

Nous arrivons à la fin de la séance. Je vais ajouter un élément.

En ce qui concerne la première question, je vais vous donner mon opinion personnelle, je pense qu'on devrait recevoir des points de situation tous les trimestres parce que de manière générale, cela nous donne un bon aperçu de ce qui se passe. Les choses évoluent très vite et à très grande échelle. Voilà, c'est juste mon point de vue par rapport à ce point.

Deux points importants. Demain à 9 h, nous aurons une séance à micro ouvert. Désolé, je vais passer quelques annonces maintenant. Soyez préparés pour demain parce que la communauté pourra nous poser tout type de questions. Soyez préparés, voilà un premier point.

Ensuite., j'ai entendu des rumeurs par rapport à des bières portoricaines qui seraient très bonnes, donc il faudra tester tout cela.

Merci beaucoup Alan, merci beaucoup Martina, Laureen et bien sûr mon vice-président. Je suis un petit peu jaloux de votre équipe d'analyse de données. J'aimerais beaucoup avoir une équipe comme cela au sein du GAC. Il faut qu'on en parle. Nous pourrons commencer les négociations je pense et voir comment ça se passe.

Profitez bien des leçons de salsa ce soir et profitez bien de l'hospitalité de Porto Rico. La séance est levée.

[FIN DE LA TRANSCRIPTION]