ICANN81 | Réunion générale annuelle – Discussion du GAC sur l'atténuation de l'utilisation malveillante du DNS
Mardi 12 novembre 2024 – 10h30 à 12h00 TRT

DAN GLUCK : Mesdames et Messieurs, nous allons commencer. Veuillez s'il vous plaît prendre place. Bonjour et bienvenue à cette discussion du GAC sur l'abus du DNS ce 12 novembre à 10 h 30. Je suis Dan de l'équipe de soutien du GAC.

Sachez que cette séance est enregistrée et qu'elle est régie par les normes de comportement requises par l'ICANN et la politique antiharcèlement de la communauté de l'ICANN. Les questions et les commentaires seront lus s'ils sont soumis dans la fenêtre de chat. L'interprétation pour cette séance sera dans les six langues des Nations Unies, plus portugais.

Si vous souhaitez parler pendant la séance, levez votre main sur Zoom. Parlez lentement et dites votre nom et la langue dans laquelle vous allez parler, si ce n'est pas l'anglais. Nous vous rappelons que les tables avec un microphone sont réservées aux membres du GAC et aux invités. Maintenant, je vais passer la parole à Nico Caballero, président du GAC.

NICOLAS CABALLERO: Bonjour et bienvenue à cette séance sur l'abus du DNS. Nous avons le privilège d'avoir Martina Barbero de la Commission européenne, Owen Fletcher, du gouvernement des États-Unis et Hajime Onga du Japon.

J'espère avoir bien prononcé votre nom de famille. Et nous avons l'honneur d'avoir des invités : Mahmut Esat Yildirim, de l'Autorité d'éthique de Turquie, et Leticia Castillo du département de Conformité contractuelle de l'ICANN, Reg Levy de Tucows, Dennis Tan Dan de VeriSign et Jeff Bedser de CleanDNS DNS.

Bonjour à tous ! Bienvenue à tous ! Je vais directement passer la parole à M. Hajime Onga du Japon, qui va nous présenter les détails et les nuances des discussions que nous aurons aujourd'hui.

HAJIME ONGA : Merci beaucoup. Bonjour à tous ! Onga Hajime au micro. Je m'appelle Onga Hajime. Je suis représentant du GAC du Japon.

Cette séance va être dirigée par le Japon, les États-Unis et la Commission européenne. Pendant cette session, nous allons écouter l'expérience du gouvernement de Turquie. Nous allons écouter également les expériences de la CPH et de l'ICANN -- et du SSAC, pardon. Voilà donc l'agenda pour aujourd'hui. Après une brève introduction, nous allons avoir une présentation du pays hôte de l'ICANN. Ensuite, le département des services de la Conformité contractuelle de l'ICANN va nous présenter des informations sur le DNS et des informations sur l'amendement au contrat de registre. Ensuite, nous aurons une discussion, une table ronde avec les membres du SSAC, du CPH et de l'ICANN. Ensuite, nous aurons une discussion au sein du GAC, et finalement nous aurons une discussion par rapport aux prochaines étapes et la possibilité d'inclure ce type de discussion dans notre communiqué.

Donc tout d'abord, nous allons parler de l'atténuation des abus DNS. C'est un sujet brûlant au Japon. Ce problème a suscité beaucoup d'attention, surtout en ce qui concerne les activités d'hameçonnage. Deuxièmement, selon le RAA et le RA, les opérateurs de registre doivent signaler des abus ou des utilisations malveillantes du DNS en vertu de leur contrat. Dans ces contrats de registre, les abus du DNS sont définis comme étant la distribution de logiciels malveillants, les réseaux zombies, l'hameçonnage, le dévoiement et le spam lorsqu'il est un vecteur pour d'autres mécanismes d'abus.

Nous allons donc parler des efforts menés par l'écosystème du DNS dans son ensemble.

Diapo suivante s'il vous plaît !

Ici, vous voyez un schéma du mandat de l'ICANN par rapport aux activités d'atténuation d'abus du DNS. Ce que vous voyez en vert, ce sont les activités de conformité contractuelle de l'ICANN, limitées aux RAA et aux RA. Ces activités menées par l'ICANN auprès des opérateurs de registre et des bureaux d'enregistrement sont celles que vous voyez sur l'écran. Les titulaires de noms, les ccTLD et les revendeurs ne font pas partie de ce chemin. Aujourd'hui, nous allons parler spécifiquement de ce qui se retrouve sur le carré vert.

L'utilisation malveillante concerne également les ccTLD. Ce type d'abus du DNS est prévalent dans l'industrie du DNS. Et vous le voyez représenté dans le rectangle bleu. Les malveillants utilisent des services comme des services d'hébergement qui sont représentés dans

la partie rouge du schéma pour atténuer les utilisations malveillantes du DNS. Nous menons des activités en collaboration.

Diapo suivante s'il vous plaît !

Le mois dernier, nous avons organisé un webinaire avec Jeff qui sera dans la table ronde de discussion, où nous avons introduit le SSAC115 qui est une référence dans ce domaine.

Dans cette présentation, Jeff a présenté un certain nombre de discussions par rapport à un cadre pour atténuer l'utilisation malveillante du DNS. Il a souligné l'importance de la coopération entre la communauté DNS dans son ensemble.

Aujourd'hui, notre séance va aborder les points que vous voyez dans l'encadré rouge. Tout d'abord, l'autorité des TIC de Turquie va nous présenter leur approche par rapport à l'utilisation malveillante du DNS. Dans le communiqué de Kigali du GAC, nous savons qu'il est très important de pouvoir tirer des enseignements d'autres régions sur des bonnes pratiques dans ce domaine. Cette présentation, donc, va nous présenter les initiatives de Turquie, y compris la coopération avec les différentes parties prenantes.

Diapo suivante. Excusez-moi. Non, pas encore. Alors ensuite, nous allons voir ce qui peut être fait au niveau de l'ICANN. Tout d'abord, l'ICANN va nous présenter les activités du département de la Conformité contractuelle au niveau des RA et RAA. Ensuite, on aura une discussion avec les parties prenantes par rapport aux effets des amendements qui ont été introduits dans les RA et RAA. Et ensuite, le

GAC va discuter des effets sur les amendements et les expériences pertinentes. Ensuite, nous allons voir ce que nous pouvons faire avec l'écosystème dans son ensemble. Dans les séances d'aujourd'hui, nous allons expliquer également quelles vont être les prochaines étapes.

Donc vous voyez quel est l'ordre du jour pour aujourd'hui? Et je demande à tous les intervenants de respecter le temps qui leur sera imparti pour leur présentation. Je vais commencer donc par présenter et donner la parole à M. Mahmut Esat Yildirim.

MAHMUT ESAT YILDIRIM : Mahmut au micro. Je suis Mahmut Esat Yildirim. Je suis le chef du département des TIC dans le BTK. Je vais vous parler des mécanismes utilisés par les CERT et par notre département en Turquie.

Diapo suivante, s'il vous plaît !

NICOLAS CABALLERO: Mahmut, est-ce que vous pourriez parler plus près du micro ?

MAHMUT ESAT YILDIRIM : Les CERT nationaux, les équipes d'intervention informatique d'urgence de Turquie, se trouvent dans le même département que notre département. Et donc, le CERT, c'est l'équipe d'intervention informatique d'urgence de Turquie. Et son rôle est d'identifier et d'atténuer les menaces d'utilisation malveillante du DNS à l'échelle du pays.

Comme je vous l'ai dit, le ccTLD, le gestionnaire du ccTLD .TR, c'est TRABIS. Et TRABIS et notre CERT sont dans le même département et ils partagent un pouvoir, celui de lutter contre les cybermenaces et l'utilisation malveillante du DNS.

Nous avons une stratégie nationale et un plan d'action national pour la sécurité cybernétique. Dans ces stratégies et ces plans d'action, il y a donc des actions pour atténuer les mécanismes d'abus et pour lutter contre les menaces cybernétiques. La dernière version de la stratégie et du plan d'action nationaux sur la cybersécurité a 4 thèmes, 6 objectifs stratégiques, 18 cibles et 61 points d'action.

Les points que vous voyez sur l'écran nous permettent de voir qu'il s'agit d'une approche basée sur l'humain, une approche orientée à l'action, résilience cyber, technologie nationale pour combattre les cybermenaces, et une marque turque au niveau international. Tout cela se trouve dans notre plan d'action et notre stratégie cyber.

Quelles sont les bases juridiques pour mener ces activités d'atténuation de cybermenaces et d'utilisation malveillante du DNS ?

Cela est mis en œuvre conformément aux articles de la loi sur les communications électroniques de la Turquie. C'est la loi 5809. Dans l'article 60, paragraphe 11, de cette loi, il est dit que l'organisation doit avoir quelqu'un qui mette en place les mesures nécessaires pour protéger et prévenir les cyberattaques aux organisations gouvernementales privées ou aux entités réelles. C'est une loi qui prévoit les responsabilités au niveau des équipes d'intervention

informatique d'urgence, et qui prévoit également les actions à mettre en œuvre en cas de cyberattaque.

Le paragraphe suivant de la même loi dit l'organisation peut recevoir et évaluer des informations, des documents, des données et des fichiers dans le cadre de sa mission. Nous pouvons, en vertu de cette loi, nous pouvons demander des informations pour détecter les cyberattaques et nous pouvons demander ces informations à différentes organisations ou à différents systèmes.

Les bases juridiques pour les ccTLD se trouvent également dans notre législation. Nous travaillons en étroite collaboration avec les forces de l'ordre et les agences d'application de la loi. Et nous fournissons les informations que nous demandent ces autorités. Parfois, nous travaillons également étroitement avec les CERT et les forces de l'ordre pour identifier et prévenir ce type d'activités malveillantes.

Alors, quelles sont les activités d'utilisation malveillante auxquelles nous sommes confrontés tous les jours ? Hameçonnage, distribution de logiciels malveillants, spam, détournement de nom de domaine, réseau zombie, parfois du matériel pédopornographique, fraudes, arnaques, abus de DNS comme par exemple différents types d'attaques techniques, des violations privées, violations de la vie privée, usurpation d'identité, usurpation du DNS. Et donc nous essayons d'identifier toute cette catégorie et nous utilisons des outils et des mécanismes pour les identifier justement.

Alors le premier de ces outils que nous avons construits s'appelle AZAD. Il s'agit d'un projet qui a été fabriqué en interne et qui utilise

l'intelligence artificielle pour détecter des domaines qui mènent des activités d'hameçonnage. Par exemple, nous recollectons toutes les informations sur les nouveaux noms de domaine et d'autres informations venant d'autres domaines. Nous recueillons donc des informations par rapport à des milliers de noms de domaines. En utilisant donc -- en mettant à profit l'intelligence artificielle, nous sommes capables d'identifier des domaines liés à des activités d'hameçonnage parmi tous ces milliers d'autres domaines. Nos opérateurs dans les ccTLD peuvent vérifier de manière manuelle si ce nom de domaine est vraiment lié à des activités d'hameçonnage. Jusqu'à maintenant, ce logiciel a eu un taux de réussite de 97 %. L'analyse, donc, nous permet d'identifier ces domaines et de les bloquer avant qu'ils ne soient actifs.

Et donc le CERT et les ccTLD, ensemble, nous travaillons étroitement en coopération avec les FAI en Turquie, afin d'agir de manière vraiment très rapide et atténuer ce type d'activités malveillantes. Toutes ces informations que nous recevons, toutes les activités liées à des plaintes en matière de cybersécurité, tous ces outils sont développés en interne. Nous recevons les différentes informations au niveau des différentes divisions que nous avons en interne. Voilà comment nous travaillons au niveau de TRABIS. Nous recueillons des signalements de différentes sources, des opérateurs de registre, bureaux d'enregistrement, utilisateurs finaux ou le système AZAD. Nous recueillons donc tous ces signalements et toutes ces informations. Ensuite, nous les renvoyons au système TRABIS. Ce sont ces ccTLD qui analysent ces notifications à l'aide de l'intelligence artificielle. Et si ces informations se confirment, ils peuvent bloquer le nom de domaine.

Voici quelques statistiques par rapport aux incidents d'utilisation malveillante du DNS. Nous avons donc recueilli plus de 13 000 plaintes. Dont 8000 étaient vraiment des incidents. Pour eux, pour nous, cela veut dire que nous devons vérifier ces signalements pour voir s'il s'agit vraiment d'une activité malveillante ou pas. Donc, de ces 8000 incidents, pardon, de ces 13 000 plaintes, 8000 étaient des cas d'abus. Donc nous avons soit annulé le domaine, soit nous avons interrompu ces activités. Nous avons trouvé plus de 9000 domaines qui menaient des activités malveillantes, 26 noms de domaines qui distribuaient des logiciels malveillants, 3 réseaux zombies, et les informations que vous voyez sur l'écran.

Il y a certaines tendances communes lorsqu'on parle des listes de noms restreints. Par exemple, peut-être qu'en anglais, cela n'a pas de sens, mais le mot plainte, annulation, tout cela peut-être utilisé pour mener des activités malveillantes. Nous, le nom banque n'est pas utilisé largement, parce que nous avons une liste restreinte de noms qui peuvent utiliser le mot banque. Et donc les acteurs malveillants ne peuvent pas enregistrer des noms de domaine liés au mot banque.

Diapo suivante, s'il vous plaît.

En Turquie, des mots tels qu'opportunité, rabais, confiance en ligne, campagne sont des noms très utilisés dans les activités malveillantes. Je répète, peut-être que cela n'a pas de sens en anglais, mais nous essayons d'améliorer nos outils basés sur l'intelligence artificielle en utilisant ce type de mots tous les jours. Nous apprenons de nouveaux mécanismes et de nouveaux mots. Nous apprenons de nouveaux mots

à ces mécanismes d'intelligence artificielle pour améliorer leurs performances.

TRABIS a été créé en 2022. Et à partir de cette date, on a constaté certains points charnières. À partir de TRABIS, nous avons changé le modèle d'enregistrement de nom de domaine. Avant, on avait des noms de domaine comme .TR, net.TR et org.TR, et pour les enregistrer, il fallait fournir des documents. Mais à partir de TRABIS, nous suivons l'ordre d'enregistrement. Et c'est pour cela que les activités malveillantes ont augmenté. Cela nous a menés à travailler à l'amélioration de nos mécanismes de dépistage. Et à partir de 2023, nous avons commencé à utiliser les capacités de CERT avec TRABIS, afin d'atténuer ces attaques.

Diapo suivante.

Nos méthodes pour envoyer des plaintes sont par mail à travers les méthodes de plaintes de CERT ou alors à travers notre page Web ou à travers notre ligne verte. Vous pouvez nous appeler pour nous signaler des activités malveillantes. Si vous accédez à notre site Web usom.gov.tr, vous verrez quelles sont les adresses qui sont sur la liste noire. Cette liste est publique ; tout le monde peut y accéder. Nous la partageons avec tout le monde pour que vous puissiez ajouter ces noms de domaine malveillants qui font des attaques de logiciels malveillants, d'hameçonnage ou autres à vos propres listes noires.

Prochaine diapo.

Donc nous sommes ouverts à la collaboration avec les membres du GAC. Ensemble, nous cherchons quelles sont les politiques les plus efficaces pour atténuer l'utilisation malveillante du DNS, et nous considérons également comment les politiques y afférentes des autres ccTLD, des autres pays, peuvent renforcer notre mécanisme, comment les intégrer à nos processus pour améliorer nos résultats. Et nous voulons nous-mêmes contribuer et apporter ce que nous avons conçu aux autres. Si vous avez des questions, n'hésitez pas. Merci.

NICOLAS CABALLERO: Merci beaucoup Mahmut. S'il y a des questions pour Mahmut, c'est le moment de les poser. Je n'en vois pas.

Je voulais moi-même vous interroger à propos du type de technique que vous utilisez, par exemple, pour identifier un trafic anormal dans le DNS ou des requêtes qui sortent du normal ou du spam en général. Quelles sont les techniques d'intelligence artificielle qui vous ont donné le plus de résultats ? Ou alors suivant vos résultats dans ces cas-là, comme le Random Forest ou *deep learning*, dans ces cas-là, quels sont les réseaux neural que vous utilisez ? Je ne veux pas entrer trop dans les détails techniques, mais est-ce que vous avez une idée générale de ceux qui fonctionnent le mieux de votre point de vue et en fonction de vos expériences ?

MAHMUT ESAT YILDIRIM : Très bonne question. J'adore les aspects techniques. Alors, dans ce processus d'apprentissage automatique, nous avons deux aspects. Il y

a les méthodes d'apprentissage automatique pour identifier les similarités entre les noms de domaines récemment enregistrés. Par exemple, moi j'ai enregistré mahmut.com et nos modèles d'apprentissage automatique vont vérifier s'il s'agit d'un site conçu à des fins d'hameçonnage à 90 % près.

NICOLAS CABALLERO: Donc Random Forest ?

MAHMUT ESAT YILDIRIM : Oui. En termes généraux. Mais nous travaillons de près avec les FAI et avec le CERT, qui utilisent leur propre système pour identifier d'autres types d'abus de DNS, par exemple, le détournement d'un nom de domaine ou des attaques techniques sur les réseaux. Et ils utilisent d'autres modèles d'apprentissage automatique pour pouvoir dépister ces paquets. Quand les FAI identifient de telles attaques, ils vont nous informer et à ce moment-là, avec les experts du CERT et du ccTLD, nous agissons pour répondre à ces incidents afin d'atténuer les attaques aussi. Merci.

NICOLAS CABALLERO: Merci. J'ai la Commission européenne et puis Mustafizur. Commission européenne.

GEMMA CAROLILLO : Merci. Gemma Carolillo, de la Commission européenne. Merci, Nico, et merci aux collègues de la Turquie pour cette présentation très intéressante.

J'ai quelques questions au sein de l'Union européenne pour notre propre ccTLD, le .EU, nous avons une approche très similaire. On utilise l'intelligence artificielle et l'apprentissage automatique dans l'étape de prévention pour empêcher l'enregistrement de noms de domaine malveillants. Votre approche semble aller au-delà et c'est très intéressant. Si j'ai bien compris, vous intégrez l'intelligence, les renseignements par rapport aux menaces à partir du CERT. Et donc, vous allez au-delà de l'étape de prévention au moment de les identifier. Vous répondez, si j'ai bien compris.

Et puis je ne sais pas si vous avez des informations à partager, si vous pouvez les partager. On a beaucoup discuté de ces outils au sein de notre groupe, et vous dites que c'était développé [internement] par votre ccTLD. Avez-vous des informations par rapport au coût d'un tel système et croyez-vous que ces systèmes pourraient être ouverts, s'ils pourraient être facilement intégrés à d'autres opérateurs de registre ? Merci.

MAHMUT ESAT YILDIRIM : Merci. Alors généralement, pour nos mécanismes de CERT, nous avons nos propres développeurs qui ont des activités en interne. Ça leur a pris à peu près un an [de] développer ce mécanisme, et ça aurait pu prendre un peu moins de temps peut-être. Mais ça a pris plus d'un an que d'apprendre aux algorithmes d'apprentissage automatique à créer ces

nouveaux modèles. Avant de développer ce logiciel, nous avions des opérateurs qui étiquetaient les noms de domaine manuellement. Et alors à ce moment-là, ils disaient c'est de l'hameçonnage, c'est du logiciel malveillant, etc. Et avec cette liste de domaines, à partir de cette liste, nous avons pu créer de nouveaux modèles que nous améliorons au quotidien. C'est pour cela qu'on a eu un taux de réussite aussi élevé.

Par ailleurs, avec le mécanisme CERT, comme vous l'avez dit, on peut empêcher directement les activités malveillantes. Le ccTLD peut identifier les activités malveillantes ou quelqu'un peut nous le signaler aussi. Parce qu'on a un site Web où les utilisateurs peuvent nous envoyer leur signalement et, en coopération entre les FAI et les CERT, on peut bloquer l'accès à ce nom de domaine en cinq minutes. On peut annuler les noms de domaine aussi, on peut les mettre en suspension, on peut les bloquer tout court. Cela varie en fonction des cas. S'il s'agit d'une attaque de zombie de contrôle, nous allons le bloquer directement au niveau du FAI.

NICOLAS CABALLERO: Merci Mahmut. J'ai deux autres questions. On ne va pas non plus charger Mahmut avec toutes nos questions. On pourrait en avoir des milliers. J'ai le Bangladesh et puis l'Inde, mais je vous demande de bien vouloir être brefs.

MUSTAFIZUR RAHMAN : Mustafizur au micro, du Bangladesh. Merci pour cette présentation Mahmut.

Dans votre présentation, vous disiez que la quantité de plaintes s'était réduite une fois que vous avez vérifié la documentation. Cette vérification de documents prend du temps, mais les clients s'attendent à un service rapide. Alors, comment faites-vous pour trouver un compromis entre ces deux besoins ?

MAHMUT ESAT YILDIRIM : Alors ça, c'était avant TRABIS. Comme vous le dites, à partir de 2022, le processus s'est accéléré. Avant 2022, c'était lent. On essayait de s'enregistrer dans un nom de domaine .com.TR, on envoyait ses documents officiels. Il y avait quatre ou cinq pages. Et les opérateurs devaient vérifier s'il s'agissait de documents valides ou frauduleux à travers différents mécanismes et, suite à la vérification, ils pouvaient vous permettre d'enregistrer votre nom de domaine. Mais à partir de 2022, ce n'était plus le cas. On n'exige plus de documentation. Merci.

NICOLAS CABALLERO: Merci. Il y a un téléphone qui sonne quelque part dans la salle. J'ai l'Inde maintenant. Allez-y.

T. SANTOSH : Merci. Je suis T. Santosh. Merci, Mahmut, pour cette présentation.

Je voudrais savoir si le .TR est ouvert au monde. Et si oui, quelle est la validation de vérification pour les candidats du reste du monde.

MAHMUT ESAT YILDIRIM : Alors, le .TR est ouvert à tout le monde. Cependant, il y a une quantité limitée de bureaux d'enregistrement qui sont accrédités, qui sont en Turquie. Donc vous pouvez enregistrer votre nom de domaine exclusivement à travers ces bureaux d'enregistrement qui sont accrédités. Il faut que vous ayez les données requises correctement enregistrées. Vous devez fournir les bonnes données, l'adresse physique, adresse email, etc. C'est très similaire au cas du .com ou d'autres gTLD.

NICOLAS CABALLERO: J'ai une dernière question très rapide. Je sais que je ne pourrais plus vous poser cette question après. Mais avant de céder la parole à Owen Fletcher, je me permets de vous poser cette question. Pour les tunnels DNS, qu'est-ce qui a le mieux fonctionné selon vous ? La perception en plusieurs couches pour les réseaux neuronaux ou autres dans ce contexte.

MAHMUT ESAT YILDIRIM : Dans ce contexte, avec ce flux de données, les réseaux neuronaux pourraient être le meilleur choix, me semble-t-il. On ne peut pas être sûr des mécanismes internes qui sont déployés pour ce tunnel DNS. On ne peut pas savoir ce qu'ils envoient à travers ces tunnels. Peut-être qu'on pourrait réunir ces paquets avec les réseaux neuronaux pour apprendre à la machine à identifier les tunnels DNS, les grands paquets, je veux dire, et puis on peut analyser tout cela dans les détails, à la main.

NICOLAS CABALLERO: Merci. J'ai le Bangladesh et puis je cède la parole aux États-Unis. Le Bangladesh ? Allez-y. Ah pardon, pardon, pardon. C'est une ancienne demande d'intervention. Mais j'avais vu quelqu'un qui levait la main, c'était la Libye ? Allez-y.

KHALED ALTARHUNI : Merci. J'ai une question pour Mahmut. Merci pour cette présentation. Je voudrais savoir si le système travaille dans le contexte des contenus illégaux?

MAHMUT ESAT YILDIRIM : Oui, en fait, ce logiciel que nous avons conçu, AZAD, vérifie la similarité entre le nom de domaine et les contenus du site Web aussi. Je ne l'ai pas dit pendant ma présentation. Donc d'abord, ça va sonner l'alarme s'il identifie à travers la vérification de similarité que le nom est similaire à un autre, parce que 95 % des fois il s'agit d'un DNS malveillant. Alors, ça va sonner une alarme. Mais dans ce logiciel, on ne fait pas de vérification de contenu. Ou s'il n'y a pas de contenu sur ce site qui a été enregistré, on ne peut rien faire. Si quelqu'un a un revolver entre ses mains, ça ne veut pas dire qu'il va tirer sur quelqu'un. Donc on ne peut pas voir qu'il y a une activité malveillante sur ce site Web. Mais l'algorithme va vérifier les contenus du site Web, s'ils sont renouvelés ou si le site est mis à jour. Et à ce moment-là, on peut voir s'il y a effectivement une activité malveillante réelle dans les contenus du site Web, comme un cas d'hameçonnage ou autres, et à ce moment-là, nous prenons des mesures.

NICOLAS CABALLERO: Merci, Mahmut, et merci à la Libye. Je vais maintenant céder la parole à Owen Fletcher des États-Unis. Désolé de vous avoir fait attendre. Vous avez la parole.

OWEN FLETCHER : Owen Fletcher des États-Unis ici. Merci. Je crois qu'on est un tout petit peu en retard par rapport à ce qu'on avait prévu pour cette séance. Je serai très, très bref. Et je suis sûr que les intervenants qui n'ont pas encore présenté le seront aussi. On a Leticia Castillo du département de Conformité contractuelle de l'ICANN qui nous parlera des amendements au contrat qui ont été apportés pour mieux prendre en charge l'utilisation malveillante du DNS, qui ont suivi les recommandations du GAC et de la communauté en général. Nous les avons déjà salués, mais je vais lui céder la parole.

LETICIA CASTILLO : Merci. Je suis Leticia Castillo. Je suis directeur de conformité contractuelle de l'ICANN. Et comme Owen l'a dit, je vais vous informer de nos travaux au cours des six premiers mois d'application des nouvelles exigences en matière d'utilisation malveillante du DNS, qui sont entrées en vigueur le 5 avril.

La semaine dernière, le 8 novembre, nous avons publié un rapport détaillé sur les six premiers mois d'application de ces mesures, un rapport de 17 pages qui contient énormément d'informations à propos des recherches, des enquêtes, des résultats, des exemples de réponses,

des actions qui étaient considérées en conformité et compatibles. Donc, consultez le rapport si vous êtes intéressés par les actions de l'entreprise.

Alors, passons directement aux données. Diapo suivante. Merci.

Entre le 5 avril 2024 et le 5 octobre 2024, nous avons entrepris 192 enquêtes avec les bureaux d'enregistrement et les opérateurs de registre pour enquêter sur des cas d'utilisation malveillante du DNS. Et c'était des cas où il y avait au moins un type d'attaque qui sont les réseaux zombie, l'usurpation, le détournement, l'hameçonnage, qui étaient utilisés pour finalement abuser le DNS d'une manière ou d'une autre.

Le résultat de ces enquêtes, nous avons fini par déléguer deux cas à l'opérateur de registre avec une note d'enfreinte formelle et un cas à un bureau d'enregistrement pour manque de conformité avec les exigences des nouveaux amendements au contrat. Et nous avons nous-mêmes résolu 154 enquêtes à travers l'étape de résolution informelle de notre processus, qui est un processus dans lequel nous pouvons résoudre la plupart des plaintes et des signalements de tout type, parce que les opérateurs de registre ou les bureaux d'enregistrement montrent être en conformité ou alors prennent des décisions pour remédier à un manque de conformité avant que cela soit délégué ou avant que l'on prenne des mesures de conformité.

Une affaire de conformité peut impliquer un nom de domaine ou plusieurs. Et une enquête en matière de conformité par rapport à une certaine quantité de noms de domaine peut mener à la découverte de

plusieurs noms de domaine malveillants sous un même compte. Et donc ces 154 enquêtes qui ont été résolues ont mené à la suspension de plus de 2700 noms de domaine malveillants et à la suspension de plus de 350 sites Web. Et dans ce cas-là, c'est parce que le bureau d'enregistrement ou le revendeur était également le fournisseur de services d'hébergement pour ces noms de domaine.

Je signale en même temps que ces statistiques correspondent à nos six premiers mois, du 5 avril au 5 octobre. Actuellement, nous avons d'autres enquêtes en cours et des centaines de noms de domaines qui sont sous la loupe. D'autres ont été fermés à partir du 5 octobre, mais ne font pas partie de ces statistiques. Cela sera inclus dans nos mises à jour futures. Pendant ces six premiers mois, nous avons également participé à plusieurs activités de sensibilisation avec la communauté pour pouvoir la mettre au courant des nouvelles exigences. Par exemple, au mois de septembre, nous avons participé à un atelier avec les parties contractantes à Beijing, où nous nous sommes concentrés sur ces nouvelles exigences en matière d'utilisation malveillante du DNS. Et le mois dernier, on était ici à Istanbul, où nous avons beaucoup travaillé avec nos collègues de GDS et du GSC pour organiser ce type d'activités de renforcement des compétences dans le cadre du Programme d'atténuation de l'utilisation malveillante de l'ICANN.

Nous venons de lancer un audit qui vise à valider la conformité des opérateurs de registre avec les exigences du RA, y compris l'utilisation malveillante du DNS. Ce n'est pas exclusif, mais ça les inclut. Et nous avons commencé à publier des rapports mensuels, à partir du mois de juin, à propos de l'application de nos exigences. Ces rapports détaillent

le type d'activités malveillantes et les activités d'application y afférentes. À partir d'avril, on a commencé avec les données du mois d'avril. Et nous mettons à jour ces rapports mensuellement. Le format que nous utilisons fournit un panorama exhaustif de ces cas-là. Nous le croyons au moins, et nous ajoutons à cela des mises à jour périodiques avec les résultats et les informations d'intérêt. L'idée est toujours de continuer à les améliorer en permanence. Donc, si la communauté avait des retours nous permettant de le faire, nous en serions reconnaissants. Le rapport du 8 novembre est accessible à partir du lien que j'ai ajouté sur cette diapo.

Diapo suivante.

Je vous disais avant qu'il y a eu 151 cas d'abus du DNS qui ont été résolus. Ici, vous voyez les raisons pour lesquelles, comment, pourquoi ces cas ont été résolus. Vous avez donc les chiffres sur l'écran. 52 % des cas, dans 52 % des cas, le Bureau d'enregistrement a confirmé l'abus et a mis en place des mesures pour suspendre ces activités. Dans environ 21 % des cas, le bureau d'enregistrement n'a pas trouvé des preuves exploitables d'abus du DNS, et la réponse était une explication raisonnable selon laquelle ils nous disaient ce qu'ils avaient fait pour investiguer le cas. Et cela a conclu donc la -- a résolu la plainte. Par exemple, ils avaient évalué toutes les informations concernant le nom de domaine, y compris des informations comptables, des discussions avec les bureaux d'enregistrement, et ils ont déterminé que le titulaire de nom était donc vraiment la personne qui utilisait le nom de domaine. Dans environ 12 % des cas, le bureau d'enregistrement a pris des mesures pour interrompre l'utilisation malveillante du DNS. Par

exemple, un titulaire de nom, par exemple, en bloquant l'URL qui menait au site malveillant, le titulaire de nom était en train de mener l'activité malveillante. Il y a d'autres mesures qui ont été prises, par exemple en détournant l'adresse DNS pour que l'activité malveillante puisse être détournée vers des adresses qui sont contrôlées par le bureau d'enregistrement.

Nous avons résolu trois cas d'abus du DNS avec les opérateurs de registre. Dans ces trois cas, les noms de domaine ont été suspendus par l'opérateur de registre. Ces cas ont été résolus, mais nous en avons d'autres qui sont encore en cours. Nous avons eu un cas qui se limitait à des problèmes concernant les informations de contact. Et ce cas-là a été résolu. La différence de chiffres entre les cas résolus entre les bureaux d'enregistrement et les opérateurs de registre tient au fait que de toutes les plaintes reçues, 54 % concernaient des bureaux d'enregistrement. Mais nous n'avons pas un seuil maximum pour lancer des investigations. C'est pour ça que, dans cette période, nous avons envoyé plus d'avis de manquement aux bureaux d'enregistrement qu'aux opérateurs de registre. Je vous ai dit que ces chiffres correspondent à cette période. Nous avons encore d'autres cas qui ont été résolus après le 8 octobre, et nous allons donc continuer à faire des états de situation et à publier des rapports avec les détails des autres cas qui ont été résolus après le 8 novembre.

Je vais m'arrêter ici et répondre à vos questions si vous en avez.

OWEN FLETCHER : Merci beaucoup. Je trouve les informations que vous avez données très utiles. Il s'agit d'un sujet très important pour le GAC, et je suis sûr qu'il y aura des questions de la part des membres du GAC. Nico, on a le temps ?

NICOLAS CABALLERO: Nous avons le temps pour quelques questions. L'inde, s'il vous plaît.

T. SANTOSH : Cette présentation nous a permis de comprendre mieux le rôle des bureaux d'enregistrement et des opérateurs de registre. En Inde, nous avons eu trois plaintes de ce type par le biais de notre site Web de plaintes en matière de conformité contractuelle, mais nous n'avons aucune statistique par rapport à ce type de plainte. Alors, quel est l'état de situation des différentes plaintes ?

LETICIA CASTILLO : Si j'ai bien compris, vous avez signalé trois -- vous avez déposé trois plaintes et vous n'avez pas l'état de situation de ces plaintes. C'est bien ça, votre question ? Je crois que je suis au courant des plaintes dont vous parlez, et je crois que nous avons demandé de retour certaines informations dont nous avions besoin, et que nous avons demandé à disposer davantage de temps pour pouvoir revenir vers vous. Mais bien évidemment, je peux m'en informer et revenir vers vous pour vous dire où nous en sommes.

Donc, une fois que la plainte est déposée, il y a une confirmation avec un numéro de cas qui est attribué. Ensuite, il y a des communications

supplémentaires qui peuvent être envoyées à la personne qui a déposé la plainte en demandant des informations supplémentaires, par exemple, ce qui arrive souvent. Parfois, nous avons besoin de clarifications. Nous avons besoin davantage de preuves. Une fois que nous recevons ces informations, des cas comme l'exemple que je vous ai donné. Parfois, nous avons besoin de donner plus de temps aux plaignants pour qu'ils nous envoient cette information. Et quand le cas est résolu, le plaignant reçoit une explication par rapport à la manière dont le cas a été résolu. Et nous envoyons toujours des informations de contact à chaque plaignant.

Donc voilà un petit peu le processus, mais je serai ravie d'en parler en privé avec vous.

NICOLAS CABALLERO: Pays-Bas et ensuite les États-Unis. S'il vous plaît, soyez bref.

ALISA HEAVER : Merci pour cette présentation.

Je me demandais dans quelle mesure ces chiffres peuvent être comparés aux chiffres d'il y a un an ou un an et demi, lorsque ces amendements n'étaient pas encore en vigueur.

Deuxième question, quelle est la durée moyenne d'une investigation ou d'une enquête avant que le bureau d'enregistrement mette en place des mesures, et dans quelle mesure les investigations qui ont été lancées, dans quelle mesure elles se sont basées sur les mesures

contractuelles nouvelles par rapport aux contrats précédents qui n'avaient pas ces amendements ?

LETICIA CASTILLO : Merci beaucoup pour cette question. En ce qui concerne les chiffres, pendant les deux dernières années, même avant le 1er avril -- le 5 avril, nous avons reçu une augmentation des plaintes en matière d'abus de DNS. En 2023, nous avons reçu au total en moyenne plus de 1300 plaintes par mois. De janvier à septembre 2024, la moyenne était de 2000 plaintes. Donc il y a eu une augmentation, sans aucun doute, et même avant le 5 avril 2024.

En ce qui concerne le temps qu'une investigation peut prendre, cela dépend des cas d'abus de DNS où nous contactons le bureau d'enregistrement. Le bureau d'enregistrement nous dit oui, le nom de domaine doit être suspendu, et cela peut-être le jour même. Mais nous avons des investigations qui concernent des centaines ou des milliers de noms de domaine, où les parties contractantes nous demandent de non seulement identifier le modèle d'abus, mais d'utiliser également -- d'essayer de trouver des tendances. Et cela prend plus de temps. Nous leur demandons, dans ce type de cas, de nous fournir un plan d'atténuation avec des étapes pour être sûrs que ce processus est en place. Et nous attendons jusqu'à ce que ce processus soit en place et nous le vérifions. Et ensuite, nous le surveillons de près parce que des problèmes peuvent avoir lieu après la mise en œuvre de ce plan. Donc, tout cela pour vous dire que cela dépend des différents cas d'abus.

NICOLAS CABALLERO: Merci. J'ai encore une demande des États-Unis. Laureen, s'il vous plaît.

LAUREEN KAPIN : Je parle en tant que membre du Groupe de travail sur la sécurité. J'aimerais remercier l'équipe pour ce travail qui est fait. Et je voulais vous dire que ces informations sont très encourageantes, parce qu'on voit qu'il y a des réponses très concrètes aux cas d'utilisation malveillante du DNS. Cela est vraiment très positif.

Ma question est la suivante : il y a une catégorie, dans le schéma, une catégorie à part, où [il dit] que le bureau d'enregistrement prend des mesures pour arrêter l'abus du DNS en suspendant le nom de domaine. Pourriez-vous nous donner davantage d'informations ?

LETICIA CASTILLO : L'obligation dans le contrat, c'est de mettre en place des mesures d'atténuation pour arrêter ou interrompre l'abus de DNS. Les mesures à prendre dépendent des circonstances spécifiques. De manière générale, dans des cas très clairs d'abus de DNS, en général, le nom de domaine est suspendu, mais dans d'autres cas, comme l'exemple que j'ai donné auparavant, par exemple, dans ce cas, dans un cas particulier, il y avait un nom de domaine qui était compromis et le bureau d'enregistrement a informé le titulaire de domaine de ce qui se passait. Le titulaire s'est occupé de son nom de domaine et a trouvé une solution. Et cela faisait partie également du contrat.

NICOLAS CABALLERO: Je vais revenir vers Owen.

OWEN FLETCHER : Je suis d'accord. C'est positif de voir ces chiffres fournis par le service de conformité contractuelle. Et c'est très utile de voir donc ces résultats positifs.

Nous allons passer maintenant à une discussion en table ronde. Nous avons Reg Levy de Tucows, Dennis Tan de VeriSign et Jeff Bedser de CleanDNS et membre du SSAC. Ils vont répondre à quelques questions que nous allons voir affichées sur l'écran. Ces questions, par exemple pour Dennis en tant que partie contractante, qu'avez-vous fait depuis les amendements ? Les questions 2 et 3 sont pour tous. Quels ont été l'impact et les conséquences de ces amendements, à votre avis ? Et quels sont les apprentissages tirés de ces premiers six mois de mise en œuvre des amendements ? Nous aimerions donc en savoir plus par rapport à l'impact de ces amendements. Nous vous demandons de vous en tenir aux trois minutes qu'on vous a imparties et nous allons commencer avec Reg.

REG LEVY : Reg Levy de Tucows, bureau d'enregistrement de nom de domaine. Tucows a été très impliqué dans la négociation des amendements. Et donc nous n'avons pas changé grand-chose depuis les amendements, parce que nous faisions déjà beaucoup de ces actions. Mais nous sommes satisfaits que ces amendements soient maintenant en vigueur. Nous avons une équipe de sept professionnels des abus, qui vérifient

tous les signalements, qui vérifient donc les abus, et qui prennent des mesures d'atténuation.

Ce qui a changé depuis l'amendement, mais pas à cause des amendements, c'est que nous avons commencé à mettre des mesures de *sinkholing*, au lieu de suspendre les noms de domaine faisant de l'hameçonnage. Que veut dire *sinkholing* ? Cela veut dire que nous redirigeons les enregistrements DNS vers un domaine avec un certain nombre de serveurs DNS qui sont gérés par CleanDNS et donc ils peuvent collecter plus d'informations sur les campagnes d'hameçonnage et nous pouvons identifier des tendances. Donc, nous pouvons identifier certaines choses. Mais CleanDNS peut en tirer des tendances, et ces informations que nous leur fournissons leur permettent de mieux cibler les campagnes d'hameçonnage dans l'industrie.

OWEN FLETCHER : C'est très bien. Vous avez -- vous vous êtes tenu aux trois minutes. C'est très bien. Dennis ?

DENNIS TAN : Merci Owen. Il y a beaucoup plus à ajouter en ce qui concerne l'impact des amendements pour ce qui est des opérateurs de registre. Une grande partie de la responsabilité repose sur les bureaux d'enregistrement qui ont un lien direct avec les titulaires.

Au niveau des opérateurs de registre, nous essayons d'identifier les menaces à grande échelle, par exemple les réseaux zombies. Et cela est

important pour éviter l'enregistrement malveillant de noms de domaine. Nous utilisons de l'ingénierie inverse, au niveau de l'enregistrement.

Pour ce qui est des noms de domaine enregistrés, nous essayons donc de voir quelle est la manière dont les bureaux d'enregistrement gèrent les cas signalés.

De manière générale, et ici, je parle vraiment de manière très générale au niveau des opérateurs de registre, les amendements ont permis, du point de vue pratique, ont permis d'augmenter et d'améliorer le niveau de signalement, car on demande à avoir des preuves qui nous permettent de mieux évaluer de quel type d'abus il s'agit, et afin de prendre les mesures appropriées.

Je voudrais signaler également qu'au niveau de nos groupes CPH et le Groupe de travail sur le DNS, depuis les amendements en vigueur, nous avons dit que c'était toujours un premier pas vers d'autres activités pour atténuer l'utilisation malveillante du DNS. Nous avons mené des actions de sensibilisation auprès des communautés, de la communauté, pour voir s'il y a d'autres aspects à considérer au niveau des politiques, au niveau des meilleures pratiques, pour trouver des solutions à ces problèmes. Très récemment, certains d'entre vous avaient peut-être participé à la séance avec NSG, où l'on a passé en revue les pratiques abusives depuis l'optique des droits humains. C'est un exemple de travail que nous pouvons mener avec la communauté de l'ICANN. Je vais m'arrêter ici et je reviens vers vous, Owen.

OWEN FLETCHER : Merci Dennis. C'est très bien. On passe à Jeff maintenant, qui a préparé une présentation.

JEFF BEDSER : Oui, alors je vais sauter les premières diapos qui répètent ce qui a déjà été expliqué. Oui, la suivante encore. Voilà.

Je voudrais établir ici une comparaison au niveau des données. Je m'excuse parce que j'ai des problèmes de gorge. Donc je ferai de mon mieux pour que vous puissiez m'entendre. J'ai des données à partager à propos des volumes généraux d'utilisation malveillante du DNS, pour que vous ayez un peu plus de perspective par rapport aux volumes dont nous parlons.

La période d'avril à juin a été une période pendant laquelle nous avons traité 628 000 signalements d'abus, pour représenter 155 000 domaines uniques. Donc on avait plusieurs signalements pour les mêmes domaines souvent. Et le volume mensuel moyen avant le changement des obligations en était à 225 000 signalements par mois. Après l'intégration de ces exigences, on a commencé à recevoir à peu près 240 000 signalements par mois. Et à partir de mes discussions avec les bureaux d'enregistrement, opérateurs de registre et quelques compagnies d'hébergement, on voit une augmentation. Et je pense que c'est parce qu'on a plus de connaissances par rapport aux changements des obligations et beaucoup de personnes qui ont commencé à signaler plus ou plusieurs fois, à envoyer plusieurs plaintes pour un même incident.

Diapo suivante.

Voici encore une fois un exemple des rapports de volume entre septembre 2024 et octobre 2023. Donc on est revenu en arrière. Et vous voyez que les moyennes mensuelles augmentent parfois, se réduisent parfois aussi. Mais en moyenne, le volume est assez stable pour ce qui est de l'hameçonnage.

Diapo suivante.

Ici, j'ai inclus des données qui me semblaient intéressantes. L'opérateur de registre qui a été compromis représente une attaque publique et [départ] à propos de ce que fait l'ICANN. Pour le .TOP, nous avons vu que la notification était arrivée en juin. Et ce mois-là, il y a eu au total 7000 signalements d'abus pour le .TOP. En août, c'était de 8000, et en septembre, encore une fois, ça a augmenté de 2000. Et en octobre, de 13 000. Donc ça montre clairement que l'équipe de conformité contractuelle de l'ICANN a choisi une très bonne partie à suivre pour pouvoir contrôler cela, parce que même avec l'augmentation et la notification et le report de la date limite, le volume de signalements d'abus dans cette zone continue à augmenter aujourd'hui. Et cela ne montre pas que l'ICANN n'a pas fait son travail. C'est le fait que ce type d'intervenants, en fait, change les obligations. Et le changement d'obligation était fait pour résoudre un problème et ils ne [s'y] adhèrent pas.

Donc, nous mesurons maintenant, bien sûr, le total de rapports traités, la quantité de domaines impliqués, la quantité de rapports ou de signalements, la quantité d'actions entreprises par le service de

conformité contractuelle, par bureau d'enregistrement et par opérateur de registre et la quantité de notifications.

Sur cette autre diapo, j'ai inclus ce que nous devrions mesurer. Cela nous permettrait de mieux comprendre le changement de comportement et à partir de l'adoption des obligations, et combien de signalements ont été correctement utilisés pour l'atténuation. Avec 8 millions de signalements par an à peu près, la moitié, je dirais, ne sont pas fondées. On n'a pas suffisamment de preuves pour pouvoir agir. Ou alors ils sont mal classés, ils sont incorrects, et c'est plus nuisible que ce que ça aide. Combien de signalements sont fournis aux parties qui peuvent effectivement agir pour résoudre le problème ? Et ça a duré combien de temps, le problème que ça a généré ? Eh bien, j'adore parler de cela, parce qu'en général, le cycle de vie d'un domaine qui est utilisé à des fins malveillantes est de 48 h à peu près. Avec les technologies d'intelligence artificielle et l'apprentissage automatique, on peut agir très rapidement en l'espace de quelques minutes. On peut répondre à ces processus.

Une autre mesure qui devrait être adoptée, et je sais qu'ailleurs, à l'ICANN, dans le bureau de l'OCTO, ils y travaillent avec ces métriques pour les domaines, mais on devrait savoir quelle était l'efficacité de l'atténuation pour réduire les volumes en général. Aux États-Unis, on a tendance à penser aux limites. On prend une limite, et puis les gens vont aller au-delà. Et donc à chaque fois, il faut aller un peu plus loin pour pouvoir changer le comportement des acteurs. Combien d'efforts cela prend-il ? Qu'est-ce qu'il faut faire ? La partie qui n'est pas en

conformité, elle va faire quoi pour pouvoir aller au-delà ? Eh bien, c'est ça qu'on se demande.

OWEN FLETCHER : Pardon, vous allez devoir conclure.

JEFF BEDSER : C'est ma dernière diapo. Alors je vais résumer très rapidement. Le changement au niveau des obligations a été positif. Toutes les parties qui signalent des dommages ou la quantité a augmenté. Je vois que les acteurs qui sont problématiques ne sont pas dans notre écosystème. Ceux qui sont dans l'écosystème entreprennent des mesures, mais, en tout cas, on signale toujours les erreurs. Et je crois que, ici, ce qu'il faut penser est aux changements systémiques que représentent ces modifications. Et je crois que si ça ne fait que six mois que cela a été adopté, on voit déjà une tendance positive.

OWEN FLETCHER : Merci Jeff. L'équipe des domaines mondiaux et stratégiques de l'ICANN va aussi intervenir. Allez-y.

MUKESH CHULANI : Merci Owen. Je voulais souligner que nous croyons que l'impact sur le niveau des cas à partir de ces modifications est très positif. Cela fait six ou sept mois qu'on a adopté ces exigences. Et vous avez entendu les parties contractantes. Nous avons des rapports de conformité contractuelle également. Vous avez entendu parler des métriques d'un

spécialiste tiers. Et on voit partout des impacts positifs. On a un élan qui commence à s'accumuler. Les modifications pour l'utilisation malveillante, comme disait Dennis, n'étaient pas la seule mesure à entreprendre. C'est la première. Et donc, on peut déjà prévoir qu'il y ait une préférence, une tendance au changement. Et on s'attend à ce que ça continue.

Depuis notre point de vue, le service de conformité contractuelle est là pour faire appliquer les obligations contractuelles. Nous avons des données contractuelles qui sont très ciblées et très centrées sur ces cas qui existent. Ces dossiers qui sont créés. Mais ça devrait être complété par une vision un peu plus générale de l'abus sur le marché.

Nous avons des projets en cours à travers notre équipe OCTO. On a d'une part une plateforme de mesures de données qui s'appelle Metrica et on devrait en entendre parler davantage au cours des prochains mois. Et puis on a le rapport INFERMAL qui est une étude qui est lancée à propos des préférences des attaquants pour l'acceptation universelle, pour évaluer cela.

Comme Leticia l'a dit, nous continuons, bien sûr, à travailler pour trouver des moyens qui permettent de faciliter l'échange de meilleures pratiques à travers des plateformes comme celle-ci. Nous vous remercions donc de nous avoir invités. Merci.

OWEN FLETCHER : Merci Mukesh. Il est très utile pour nous de pouvoir entendre parler des parties prenantes de différents secteurs. Je crois que c'est ce qui nous

permettra d'échanger, comme vous dites, les meilleures pratiques et de connaître mieux les implications de ces modifications aux contrats qui, comme vous le dites, sont censés être une mesure, mais pas la seule.

Nous avons également réservé du temps pour le débat avec le reste de la salle pour des questions-réponses. Donc merci Nico. On revient vers vous.

NICOLAS CABALLERO: Merci Mukesh. Merci à tous les membres du panel, Reg, Dennis, Jeff. Merci Owen. On n'a pas de mains qui soient levées dans la salle ni sur Zoom en ce moment. Alors je vais céder la parole à Martina qui va animer le débat entre membres du GAC.

MARTINA BARBERO : On a une main qui vient de se lever.

NICOLAS CABALLERO: Effectivement. Commission européenne ?

GEMMA CAROLILLO : Merci Nico. J'ai une question très brève pour VeriSign, me semble-t-il. J'espère que vous pourrez répondre. Vous avez dit que vous envisagez de développer des politiques et vous considérez quel serait le meilleur secteur. Vous avez parlé d'échanges avec la communauté. D'ailleurs, je voudrais savoir si vous avez déjà des idées, parce qu'au sein du GAC,

nous discutons de ce même type de projet. On voudrait peut-être voir si on pourrait comparer nos notes.

DENNIS TAN : Merci, Gemma. Alors, on considère quel devrait être notre travail à l'avenir? Ce n'est pas nécessairement un processus d'élaboration de politiques. Il y a quelques mois, la communauté nous a dit que ce type de processus prenait beaucoup trop de ressources et de temps, et que ce serait mieux d'être plus ciblés sur notre travail et non pas d'entreprendre des PDP qui sont des travaux de longue haleine. Donc PDP, oui, effectivement, est une voie possible. On explore cela et on en discute avec la communauté de l'ICANN. On voudrait avoir plus d'informations. On voulait mieux réfléchir au rapport INFERMAL, d'ailleurs, qui vient d'être publié. Je ne l'ai pas lu en détail encore, mais oui, ça peut être le moteur de nos délibérations.

NICOLAS CABALLERO: Merci. Les États-Unis, maintenant.

OWEN FLETCHER : Merci. Owen Fletcher, encore une fois. Mais je voulais signaler que le Conseil d'administration nous avait proposé des séances d'observation à propos des PDP potentiels qui pourraient être créés, qui pourraient peut-être adresser des considérations plus subtiles, des modifications pour en faire un suivi. Je pense que ce serait intéressant d'avoir ce type de mise à jour. Ce n'est pas probablement une question pour les gens qui sont ici par contre.

REG LEVY : Oui, je suis là pour représenter le sous-groupe du RSG à propos de l'utilisation malveillante. Alors, comme vous dites, oui, on a organisé des séances d'écoute, qui ne sont pas nécessairement exactement les mêmes dont vous parlez -- le Conseil d'administration, mais nous avons contacté différents membres et groupes de la communauté, des groupes officiels et extraofficiels, pour savoir ce qui les intéresse, qu'ils voient les tendances qu'ils voudraient analyser, et comment nous, en tant que parties contractantes, pourrions les aider, et non pas nécessairement pour en créer un PDP. Mais on s'est déjà aligné avec l'ALAC. On espère pouvoir se réunir avec le SSAC aussi pour encore une fois en discuter individuellement, de sorte que chacun de ces groupes de la communauté puisse nous parler directement.

NICOLAS CABALLERO: Merci les États-Unis et merci Reg. Je ne vois pas d'autres mains qui soient levées. Donc je reviens vers Martina Barbero, de la Commission européenne, qui va nous présenter les prochaines étapes et les considérations que nous devrions envisager pour la rédaction de notre communiqué.

MARTINA BARBERO : Oui. Alors en fait, il nous reste deux autres parties de notre ordre du jour avant de vous libérer pour la pause du déjeuner. Je sais que vous avez faim, mais ne partez pas encore. Cela est important. Je voulais qu'on débatte de ce qui a déjà été dit aujourd'hui. Et on voulait également voir

si vous aviez des retours à partager au sein du GAC, en ce moment, si vous voudriez discuter de vos réactions à ces informations d'aujourd'hui par rapport à la mise en œuvre et l'impact des modifications au contrat et des amendements. Si vous avez des réactions ou des commentaires, ce serait un bon moment pour que vous partagiez cela.

Et on voulait, par ailleurs, voir s'il y avait des leçons qui ont été apprises de la série précédente et qui pourraient nous aider à mieux nous préparer pour la prochaine série en matière d'atténuation d'utilisation malveillante du DNS. On a un peu entendu parler des PIC et des RVC, hier, lors de notre séance avec la Chambre des parties contractantes. Je n'y étais pas, mais on a également discuté un peu de l'utilisation malveillante du DNS lors de la prochaine série, et des conclusions qui pourraient être intégrées à notre préparation pour la prochaine série.

Et puis finalement, on a eu une présentation très intéressante de nos collègues de la Turquie. Donc on se demande s'il y aurait peut-être de meilleures pratiques des ccTLD qui pourraient être considérées et qui pourraient peut-être être du matériel de réflexion pour l'espace gTLD. Donc peut-être, Nico, qu'on pourrait demander à voir quelles sont les réactions des membres du GAC là-dessus avant de passer à la considération du communiqué.

NICOLAS CABALLERO: Merci Martina. Alors vous pouvez intervenir si vous avez des questions, des commentaires ou quoi que ce soit que vous souhaiteriez partager. Nous vous céderons la parole. J'ai l'Inde. Allez-y.

T. SANTOSH : Pendant la réunion ICANN80, nous avions fait une proposition. Nous disions que le déploiement de DNSSEC devrait être obligatoire, en particulier dans les secteurs des finances et des services financiers, de la santé, du gouvernement et des télécommunications. Nous croyons que cela serait en ligne avec les mesures de sécurité mondiales et garantirait la protection des intérêts nationaux fondamentaux. Alors, qu'en pensez-vous par rapport à ce déploiement obligatoire du DNSSEC.

REG LEVY : Reg Levy de Tucows. Le DNSSEC, c'est un outil pour la sécurité des noms de domaine. Et HTTPS semble être le protocole de sécurité qui est adopté actuellement et que le marché semble vouloir. Nous offrons le DNSSEC et nous sommes toujours contents de pouvoir ajouter le DNSSEC aux noms de domaine qui sont enregistrés auprès de nous. Mais ce n'est pas vraiment une option populaire. Ce n'est pas un choix populaire. La plupart de nos clients ne semblent pas intéressés à profiter de ces outils comme du HTTPS. La plupart des navigateurs commencent à exiger le HTTPS, comme vous le savez, ce qui en plus motive les gens à l'utiliser. Je ne vois pas pourquoi on ne pourrait pas encourager certains secteurs. On me demande de ralentir. Pardon ?

Je ne vois pas pourquoi on ne pourrait pas demander à certains secteurs d'envisager d'ajouter d'autres passerelles de sécurité supplémentaires. Mais j'ai découvert que la plupart des clients ne sont

pas intéressés aux DNSSEC comme on le souhaiterait ici à l'ICANN, peut-être.

NICOLAS CABALLERO: Merci Reg. Le Royaume-Uni.

CHRIS : Je suis Chris et c'est ma première réunion ICANN. Je fais partie du PSWG. Et pour rebondir sur l'intervention de l'Inde, je voudrais dire que, d'un point de vue plus général, vendredi dernier, suivant notre présidence mensuelle du Conseil de sécurité de l'ONU, nous avons présidé une séance sur la rançon logicielle. Et il y a eu beaucoup d'États membres de l'ONU qui avaient signé une déclaration sur l'impact de ces pays et du secteur de la santé. Alors, je crois qu'il y a beaucoup de membres du Conseil de sécurité de l'ONU, en tout cas, qui ont un intérêt croissant là-dessus et ça dépasse le concept de sécurité. D'ailleurs, ça s'applique aussi à d'autres organismes. Et nous sommes très actifs au Royaume-Uni dans ce travail. Donc, je pense qu'il y a d'autres organismes multilatéraux qui commencent à accorder plus d'importance à ces considérations. Et le fait que le Conseil -- le fait que le Conseil de sécurité ait discuté de cette question, ce mois, génère plus d'emphase. Et peut-être qu'à travers le PSWG, on devrait également rediriger ces efforts, pour faire en sorte que l'on se penche en particulier sur ces secteurs [inaudible] en particulier. Merci.

NICOLAS CABALLERO: Merci beaucoup, Royaume-Uni.

OWEN FLETCHER : Je voulais répondre brièvement par rapport à la question concernant le DNSSEC. Si je ne m'abuse, à l'ICANN81, nous avions ajouté un texte par rapport à cela. Et c'est pour répondre à votre question, Santosh. Nous pouvons revoir ce texte. Mais je pense que, ce qu'on disait à l'époque, c'était que nous soutenions la promotion de la mise en place de DNSSEC. Cela m'a l'air bien. Je ne suis pas sûr de pouvoir accepter que l'on suggère que le DNSSEC devienne obligatoire. Je devrais, bien sûr, consulter si cela pourrait être faisable ou pas.

Je me souviens également que le SSAC, dans notre réunion bilatérale où nous avions abordé cette question, ils avaient dit que nous pouvions les contacter si nous voulions davantage d'informations par rapport à cela.

NICOLAS CABALLERO: Merci beaucoup, États-Unis. Je ne vois pas d'autre main levée ni en ligne ni dans la salle. Je vais redonner la parole à Martina Barbero, de la Commission européenne, pour voir quelles sont les prochaines étapes concernant notre communiqué. Vous avez la parole Martina. Merci beaucoup.

MARTINA BARBERO : Merci, Nico, merci à tous les membres qui ont parlé aujourd'hui. Comme cela a été dit, nous devons faire en sorte que ce sujet figure un peu plus haut dans l'ordre du jour des différents pays.

Nous allons maintenant voir ce que nous pouvons faire au niveau du communiqué. Les responsables thématiques peuvent, bien sûr, proposer des thèmes, mais ce sont les membres du GAC qui doivent finalement fournir des textes que vous suggérez d'ajouter dans les sujets d'importance, donc ce que nous pouvons inclure dans le communiqué à partir des présentations que nous avons eues sur la mise en œuvre des amendements contractuels et la mesure de leur efficacité.

Nous pourrions suggérer, par exemple, que ces activités se poursuivent. Ce serait intéressant pour nous. Et ensuite, on a entendu les membres de l'ALAC dire qu'il y a certaines attentes par rapport à un travail ultérieur au niveau des politiques. Je vous rappelle qu'il y a eu une consultation publique pour les amendements. Et à ce moment-là, le GAC avait dit qu'il y avait d'autres sujets qui pourraient faire l'objet d'un travail plus poussé. Il y a une liste ici : transparence, révision périodique des techniques d'abus du DNS, voir l'abus de DNS en dehors de l'ICANN, des considérations en matière de conformité contractuelle. Désolée, je parle trop vite. Et donc, voilà certaines thématiques qui étaient incluses dans la réponse que le GAC a fournie à la consultation publique à Kigali.

Et hier, nous avons également abordé cette question pour la préparation de la prochaine série de nouveaux gTLD. Donc, tout cela peut faire partie du communiqué. Et donc, dans les huit prochaines minutes, je voudrais savoir si ce sont des thématiques que vous considérez comme pertinentes ou si vous avez d'autres thématiques à proposer avant de commencer l'élaboration de notre communiqué.

NICOLAS CABALLERO: Merci beaucoup Martina. Le micro est ouvert. Y a-t-il des commentaires, des réactions, des questions ? Les États-Unis.

OWEN FLETCHER : Owen Fletcher, représentant des États-Unis. Nous avons dit tout à l'heure qu'il y a un rapport INFORMEL. Et peut-être que c'était Jeff qui a parlé du rapport de la plateforme Metrica de l'OCTO. Nous pouvons signaler notre intérêt à obtenir d'autres sources, des informations de ces autres sources d'information. J'ai parlé également d'autres séances qui ont lieu aujourd'hui. Et Reg a dit que les parties contractantes souhaitaient avoir plus d'informations par rapport à cela. Nous pourrions donc noter cet intérêt dans notre communiqué.

NICOLAS CABALLERO: Commission européenne.

GEMMA CAROLILLO : Je voulais rebondir sur ce qu'Owen vient de dire. Nous pourrions réfléchir aux séances que l'on a eues aujourd'hui et hier. Il y a beaucoup d'intérêt de la part du GAC à en savoir davantage du rapport du SSAC, y compris l'impact de tout cela sur l'abus de DNS. Et je pense également que la proposition de l'ALAC de travailler de manière conjointe a été très bien accueillie, notamment en ce qui concerne le signalement d'enregistrements malveillants de nom de domaine. Je pense que cette problématique en général est une inquiétude partagée pour l'ALAC et pour nous.

NICOLAS CABALLERO: Merci beaucoup, Commission européenne. Y a-t-il d'autres questions ou commentaires ? Oui, allez-y.

SAMANEH TAJALIZADEHKHOOB : Merci pour ces présentations. Je suis Samaneh, directrice de recherche au bureau de l'OCTO de l'ICANN. Puisque le nom de notre plateforme a été mentionné à plusieurs reprises, je voudrais donc faire référence à cette plateforme INFERMAL. Et je voudrais vous inviter à notre séance à 1 h 15, une séance sur l'abus du DNS, où nous allons vous présenter le travail qu'on a effectué et les prochaines étapes.

NICOLAS CABALLERO: Merci beaucoup, Samaneh, pour cette invitation, mais malheureusement le GAC va commencer sa rédaction du communiqué à cette heure-là. Cela n'empêche pas les membres du GAC d'assister ou de participer à votre séance, bien sûr.

NIGEL HICKSON : Merci beaucoup ! Je trouvais que ce dialogue est vraiment très intéressant. Bien sûr, nous n'avons pas eu suffisamment de temps pour aborder cette question, mais dans d'autres réunions du GAC, lorsque nous avons parlé du RDRS, nous avons noté le dialogue qui a eu place -- qui a eu lieu, pardon, pour avoir peut-être des petits PDP, des micros PDP, pour aborder des questions très spécifiques : hameçonnage,

utilisation malveillante du DNS. Et donc les membres du GAC avaient manifesté leur intérêt par rapport à cette possibilité. Et c'est, je pense, quelque chose sur laquelle nous devrions revenir, parce qu'il y a clairement un intérêt par rapport à certaines problématiques spécifiques.

NICOLAS CABALLERO: Merci beaucoup, Royaume-Uni. On en prend note. Y a-t-il d'autres commentaires ? Je ne vois pas de mains levées dans la salle ou en ligne. Alors, permettez-moi de remercier la Commission européenne et tous nos collègues, et leur demander s'ils souhaitent prendre la parole pour un mot de la fin.

GEMMA CAROLILLO : Nous voudrions donc remercier les membres du GAC qui ont participé à cette discussion aujourd'hui. Les responsables thématiques pourraient suggérer donc du texte pour inclure dans le communiqué sous la rubrique « Questions d'importance », et nous allons donc les prendre en considération.

NICOLAS CABALLERO: Est-ce que nos invités souhaitent dire quelque chose ?

DENNIS TAN : J'apprécie cette discussion. Merci beaucoup de nous avoir invités. Reg et moi-même sommes ravis de participer à ces discussions. Les amendements ont été une première étape, et nous avons hâte de

poursuivre ce dialogue, que ce soit pour envisager la possibilité d'un PDP ou autre. Merci beaucoup.

NICOLAS CABALLERO: Merci beaucoup, Jeff, Jimmy -- Jeff, allez-y.

JEFF BEDSER : Merci pour cette invitation. Merci de m'avoir donné la possibilité de parler sur cette question.

NICOLAS CABALLERO: Mahmut, vous souhaitez dire quelque chose ?

HIJAME ONGA : Merci beaucoup pour ces discussions. C'est ma première fois et c'est vraiment très intéressant. Merci beaucoup.

NICOLAS CABALLERO : Mahmut ?

MAHMUT ESAT YILDIRIM : Merci de m'avoir donné la possibilité de partager notre expérience avec vous, et j'espère vous revoir pour continuer à échanger des informations et à échanger nos expériences.

NICOLAS CABALLERO: Nous espérons également revenir à Istanbul bientôt. La Colombie.

THIAGO DEL-TOE : Je voulais juste rappeler à ceux qui se joignent à nous que l'utilisation malveillante du DNS est l'un des points qui figurent dans nos objectifs stratégiques. Je voulais remercier également les responsables thématiques d'avoir organisé cette séance, et j'espère que nous allons poursuivre notre travail dans ce domaine.

NICOLAS CABALLERO: Merci beaucoup à tous. Cette séance est close. Je vous demande de revenir à 1 h 15 pile pour notre réunion avec le Conseil d'administration. Merci beaucoup. Et profitez de la pause déjeuner.

[FIN DE LA TRANSCRIPTION]