ICANN77 | Forum de politiques – ccNSO : Comité permanent pour l'utilisation malveillante du DNS - enquête et référentiel
Mercredi 14 juin 2023 – 13h45 à 15h00 DCA

ORATEUR NON-IDENTIFIÉ : Nous allons commencer. Claudia, s'il vous plaît, lancez l'enregistrement.

CLAUDIA RUIZ : Bonjour et bienvenue à cette séance de la ccNSO sur le comité permanent de l'utilisation malveillante du DNS. Je suis Claudia Ruiz, je travaille avec Kim et Bart et nous serons les responsables de la participation à distance pour cette séance qui est enregistrée et régie par des normes de comportement attendues de l'ICANN.

Au cours de cette séance, les questions et les commentaires soumis dans le chat ne seront lus à haute voix que s'ils sont formulés de manière appropriée, comme indiqué dans le chat. Je lirai les questions et commentaires à haute voix pendant la durée fixée par le président ou le modérateur.

L'interprétation pour cette séance comprend l'espagnol, le français et l'arabe. Cliquez sur l'icône d'interprétation dans Zoom et sélectionnez la langue que vous écouterez pendant cette séance.

Si vous souhaitez prendre la parole, veuillez lever la main dans la salle Zoom et lorsque l'animateur de la séance appellera votre nom, activez votre micro et prenez la parole. Avant de prendre la parole, assurez-vous d'avoir sélectionné la langue dans laquelle vous allez vous exprimer dans le menu d'interprétation, indiquez votre nom pour l'enregistrement et la langue dans laquelle vous allez parler si vous ne parlez pas en anglais. Lorsque vous parlez, veiller à mettre en sourdine tous les autres appareils et notifications et veuillez parler clairement et à un rythme raisonnable pour permettre une interprétation précise.

Cette séance comprend une transcription automatisée en temps réel. Veuillez noter que cette transcription n'est pas officielle et ne fait pas autorité. Pour visualiser la transcription en temps réel, cliquez sur le bouton Closed Captions dans la barre d'outils Zoom.

Pour assurer la transparence de la participation au modèle multipartite de l'ICANN, nous vous demandons de vous connecter aux séances Zoom en utilisant votre nom complet, par exemple votre nom ou votre prénom. Vous risquez d'être exclus de la séance si vous ne vous connectez pas en utilisant votre nom complet.

Et sur ce, je donne la parole à Nick Wenban-Smith. Merci.

NICK WENBAN-SMITH : Merci Claudia.

Bienvenue à tous pour cette prochaine séance concernant le comité permanent sur l'utilisation malveillante du DNS de la ccNSO. Je vous présente ici l'ordre du jour. Nous allons entendre David, Bruce, Tania et

Angela. Nous allons vous présenter une série d'actions et nous aurons des discussions aussi. Il y a deux choses que je dois ici vous dire avant de commencer cette réunion et pour que tout le monde ait le temps d'y réfléchir.

D'abord, nous voudrions que vous commenciez à réfléchir aux prochaines étapes parce qu'une des choses à laquelle nous voulons réfléchir, c'est de travailler avec la communauté et parvenir à un accord concernant les différentes activités à mettre en œuvre. Nous avons certaines idées à ce propos et nous voudrions nous assurer en parlant avec vous que nous sommes en accord avec la communauté sur ce qu'elle considère comme utile parce que, bien sûr, nous voulons être en accord avec vos souhaits et avec vos objectifs. Les choses avancent rapidement dans ce domaine ; par conséquent, il est important qu'on soit d'accord.

Deuxièmement, je voulais vous rappeler que dans la salle Zoom, nous allons faire une enquête. En tant qu'Anglais, je n'aime pas beaucoup les référendums. Ce n'est pas une enquête destinée à la prise de décision ; il s'agit seulement de connaître un petit peu votre avis sur plusieurs thèmes que nous allons aborder. Si vous pouvez prendre un petit moment pour regarder dans la salle Zoom, participer à cette enquête et répondre à ces questions, ce serait très utile pour nous. Ceci nous permettra vraiment d'avancer au cours de la séance.

Notre ordre du jour est sur l'écran, vous le voyez, je ne vais pas le lire, mais je vais donner la parole à David qui va présenter les activités du sous-groupe référentiel du DASC. C'est une série de ressources très

intéressantes, il me semble, pour la communauté pour lutter contre l'utilisation malveillante du DNS. Je donne la parole à David.

DAVID MCAULEY : Merci beaucoup. Je suis David McAuley, je participe à la ccNSO et je vais vous présenter les travaux de notre groupe de travail, le sous-groupe référentiel. Nous avons préparé ou créé une bibliothèque de référentiel et une liste d'e-mails.

Lorsque le DASC a été créé l'année dernière il y a plus ou moins un an, nous avons décidé d'avancer à travers un système de sous-groupes. Nous avons un sous-groupe dont Bruce va parler qui va diriger une enquête et il y a un sous-groupe qui s'appelle groupe référentiel dont je suis le président. Notre travail ici porte sur les référentiels, les liens, etc. Ce sera très utile pour les gestionnaires de ccTLD pour mieux comprendre l'utilisation malveillante du DNS et ses tendances et pour créer une liste de diffusion.

Ce sous-groupe va d'abord se pencher sur la création du référentiel en lui-même. Nous avons eu une réunion au mois d'août de l'année dernière. Au mois de septembre 2022, nous avons présenté quelques idées à travers la liste de diffusion. Nous avons fait cette présentation au TLD Ops, un groupe dont je vous parlerai dans un petit moment. Ensuite, nous avons travaillé sur le référentiel en lui-même. Nous avons créé les termes de référence qui allaient être utilisés pour gérer tout cela. Nous avons présenté ceci au mois de février 2023 au comité permanent.

Je vais maintenant vous parler un petit peu de la façon dont notre groupe gère le référentiel. Nous essayons de travailler sur un système d'archives. Je vais vous expliquer comment on met en liste toutes ces données, etc. En tout cas, les termes de référence ont été présentés au mois de février et nous avions l'intention de lancer notre référentiel pour la réunion actuelle. Prochaine diapositive.

Comme je l'ai dit, le comité a créé une ressource et dans nos termes de référence, nous avons créé un conseil éditorial. Il s'agit d'un groupe qui va gérer ce référentiel et qui va accepter des soumissions une fois qu'elles auront été contrôlées par le personnel. C'est un processus de participation qui existera. Puis, nous verrons si ceci est approprié pour le référentiel et à quel point ce qui est dans ce référentiel doit être retiré et archivé. C'est ainsi que cela fonctionne.

Ce conseil éditorial va se réunir deux fois par mois en fonction du travail que nous avons. Nous parlerons à la communauté de ce que nous faisons, comment nous le faisons et nous recommandons que ce conseil soit le sous-groupe référentiel en lui-même puisque nous avons l'habitude de travailler ensemble et d'organiser cette question sur le référentiel. Prochaine diapositive, s'il vous plaît.

Sur cette diapositive qui est impossible à lire, bien sûr, l'objectif est de vous montrer le référentiel, cette bibliothèque d'informations, comment soumettre les informations. Nous allons envoyer cela dans notre annonce lors de l'ouverture du référentiel et il y aura aussi un code QR comme vous le voyez. Il s'agit des informations concernant ces ressources dont nous parlons, quel est le thème, quelles sont les

catégories d'information que l'on va avoir, comment l'on peut soumettre quelque chose lorsqu'on veut que ce soit considéré par ce groupe, ce type de chose. Cela sera présenté à la communauté sous peu.

Une autre diapositive un peu plus simple est destinée au référentiel en lui-même. Ici, vous voyez que dans le cadre des présentations et des rapports concernant l'utilisation malveillante du DNS et son atténuation, il y aura différents commentaires, articles, tout ce que nous allons utiliser, un code QR, tout ce qui va vous donner accès à ces ressources. De nouveau, ce sera annoncé formellement sous peu.

Dans un petit moment, on va commencer notre enquête, notre questionnaire, mais je voudrais d'abord résumer ce qu'est ce référentiel. Comme je l'ai dit, ce que nous allons faire, c'est mettre en place des choses qui vous permettront de regarder, de consulter et d'avoir des informations tout de suite et de savoir de quoi il s'agit, s'il s'agit de logiciel malveillant, s'il s'agit de telle ou telle autre chose, s'il s'agit d'un outil qui peut vous aider, s'il s'agit d'un article qui peut vous aider ; voilà ce type de choses que nous voulons mettre en place et que nous voulons maintenir actualisé.

Par conséquent, je voudrais maintenant commencer notre questionnaire. La première question : dans quelle mesure pensez-vous vous vous rendre sur le référentiel pour obtenir ces informations ? Très probable, probable, peu probable, pas du tout probable. Je vous laisse répondre.

Un grand pourcentage des réponses indique que probablement, ils vont utiliser ou très probablement ils vont utiliser cet outil et un peu moins de 3 % pour peu probable et un peu moins de 10 % pour probable. Je vois donc qu'il y a un espace pour cet outil. Une fois qu'il sera lancé, nous verrons quelle est la réaction au niveau de la participation de la communauté et nous verrons si cet outil est utile ou pas.

J'ai une autre question ici : est-ce que vous souhaitez fournir des contenus à ce référentiel ? Je l'ai déjà dit, ce serait simple de fournir ici des contenus pour ce référentiel et la réponse est oui, non ou peut-être. Fournir des contenus, presque 60 % ; environ 30 % ont dit que peut-être ils enverraient du contenu. J'apprécie ces informations, je crois que cela peut être utile de nous informer vraiment à mesure que nous élaborons cette ressource. Prochaine diapositive.

Voyons un petit peu l'approche concernant ce référentiel et l'opinion de la communauté. Nous allons avoir de nouveau une enquête. Je voudrais voir un peu quelle est la portée de cette ressource. Notre objectif est de fournir des ressources et des outils utiles à la communauté. Une des choses que nous ne faisons pas, c'est de créer des politiques ou des normes de comportement. Ce que nous voulons aussi, c'est que cette ressource soit appropriée pour la ccNSO. Ce n'est pas une ressource qui vise à montrer du doigt ou à faire des critiques. Cet article que je vous présente ici en particulier – je vais vous l'expliquer et parler de son contenu – est probablement un bon test pour savoir si ce référentiel est une bonne chose, s'il est approprié.

Au sein de notre sous-groupe, nous avons analysé cette question. Nous n'avons pas le temps de vous montrer des exemples. Voilà un petit article, ce n'est pas un blog, c'est un article de CircleID qui a été posté au mois de mai. Vous voyez que l'on indique qu'il y a eu une baisse importante des domaines qui ont souffert d'hameçonnage. C'est intéressant de voir ces résultats ici. À notre avis, ce référentiel ne veut pas faire ce type de chose. Cet article, par ailleurs, montre qu'il y a une conséquence concernant un procès et que cette conséquence est une baisse du hameçonnage. Ceci fournit des informations liées à l'utilisation malveillante du DNS, mais nous verrons si c'est exactement ce que nous voulons.

Comme je l'ai dit, notre conseil éditorial veut voir un petit peu ce qui est approprié comme contenu et ce que nous voulons est diffusé ici. Prochaine diapositive.

Je pensais qu'il y avait une autre question au sondage, mais si je me trompe, je vous prie de m'en excuser. Je ne vois pas la question du sondage.

ORATRICE NON-IDENTIFIÉE : Une petite seconde, je vais l'afficher.

DAVID MCAULEY : Excusez-moi. Est-ce qu'il y a des réactions ? Est-ce que quelqu'un souhaite intervenir là-dessus ? Vous êtes tout à fait les bienvenus. D'ailleurs, je vais vous montrer dans un instant une image des membres

du groupe. Nous sommes ouverts, nous avons besoin de vos commentaires.

La question est la suivante : pensez-vous que le contenu de l'article que je viens de vous montrer est approprié pour ce référentiel ou pensez-vous qu'il est trop atténué ? Cette information va être particulièrement importante pour nous. Approprié, pratiquement 70 % ; trop d'atténuation 5 % ; et pas sûr, le reste. Ceci nous aide. On va refaire un sondage à la prochaine réunion parce que c'est réellement important pour nous de connaître votre avis.

Voilà les six membres qui siègent au comité. Contactez-nous, donnez-nous vos commentaires, qu'ils soient positifs ou pas, ceci nous intéresse.

J'aimerais brièvement parler de la liste de diffusion dédiée. Je vais essayer de m'en tenir au temps qui m'est imparti. Excusez-moi si je ne détaille pas tout ce qui figure à l'écran. Mais notre rôle au sous-groupe, c'est de créer une liste de diffusion dédiée dans le droit fil de la liste de la ccNSO en voyant les modèles possibles. Ce serait une liste de contacts utile pour que les gens puissent obtenir des informations sur certaines thématiques. Dans le cas de TLD Ops, c'est la sécurité.

BART BOSWINKEL : David, excusez-moi, une question. On a une question en ligne concernant le référentiel. Est-ce que vous voulez attendre la fin de votre présentation pour l'entendre ou maintenant ?

DAVID MCAULEY : À la fin. Merci.

On voulait créer cette liste de diffusion comme l'a fait TLD Ops pour essayer d'aider les gestionnaires de TLD à aborder les questions liées à l'utilisation malveillante du DNS. Si cela va être une liste fermée, en d'autres termes, on va permettre l'accès à cette diffusion à certaines personnes uniquement, à des gestionnaires ccTLD, mais on ne garantira pas l'anonymat. On va créer une liste qui va pouvoir informer les gens de ce qui est fait par rapport à l'utilisation malveillante du DNS et on aura une liste de contacts pour que les gens puissent envoyer un message aux gens qui ont de l'expérience s'ils sont confrontés pour la première fois à ce genre de problème. C'est l'objectif de cette liste de diffusion. Entre maintenant et l'ICANN78, on veut voir comment procéder et on espère pouvoir lancer cette liste de diffusion à l'ICANN78, mais voilà un peu l'objectif de cette liste.

Voilà la question : est-ce que vous aimeriez vous inscrire ou souscrire à cette liste de listes de diffusion ? Entre maintenant et l'ICANN78, on va voir qui cibler, si ce sont les exécutifs, les gens qui travaillent du côté opération ou autre ou si ce devrait être tout le monde au niveau des gestionnaires de ccTLD. Je vois qu'il y a un vif intérêt, merci.

Question suivante : est-ce que vous pensez qu'une liste de contacts dédiée vous intéresserait, c'est-à-dire les contacts pertinents, les contacts connus et autres ccTLD ? Très bien, c'est très utile. Non : juste en dessous de 10 %. Très bien, merci. Diapo suivante.

On va inviter les gens à soumettre leurs commentaires et informations par rapport au référentiel, on va faire de la publicité. On va demander à la communauté de faire de la pub pour réagir et nous dire ce qu'ils en pensent. On va se retrouver dans quelques semaines pour commencer notre travail sur la liste de diffusion dédiée dont je vous parlais à l'instant.

Encore une fois, je n'ai plus beaucoup de temps donc je vais faire une pause, Bart, et je vais vous écouter pour la question.

BART BOSWINKEL : En fait, ce n'est pas forcément une question, c'est un commentaire qui porte sur l'exemple que vous avez utilisé de CircleID. Le commentaire est le suivant de John McCormack de Hosterstats : « Vous avez besoin de toute l'information disponible d'open sources pour lutter contre l'utilisation malveillante du DNS. Il ne s'agit pas de heurter les sensibilités, il s'agit de mettre un terme à cet abus. » Je ne sais pas si quelqu'un souhaite réagir à ce commentaire.

DAVID MCAULEY : Je vais réagir d'abord.

Merci beaucoup de ce commentaire, John, on va le prendre en considération à mesure qu'on avance. On a pas mal d'expérience engrangée. Vous avez raison, bien entendu, lutter contre l'utilisation malveillante du DNS requiert autant d'informations que possible. Ce qu'il faut prendre en considération lorsque les ccTLD sont mentionnés, on va devoir agir avec une certaine finesse, vous avez raison, mais il faut

s'assurer que ce qui est au cœur de tout, c'est une information fiable. Et je le répète, ce groupe n'est pas censé pointer du doigt les autres membres. Mais vous avez raison dans votre commentaire, merci.

BART BOSWINKEL : Il y a un deuxième commentaire de Luc Seufer Namespace : « En tant que bureau d'enregistrement, il serait bon que nous ayons accès à ce référentiel. » Je ne sais pas si vous voulez répondre. Je répète : « En tant que bureau d'enregistrement, nous apprécierions avoir accès à ce référentiel. »

DAVID MCAULEY : Oui, c'est important. Comme je l'ai dit, il faut d'abord mettre en branle tout cela, comme on vous l'a décrit. Mais vous avez raison aussi. Si les ressources sont à la hauteur de ce qu'on attend, alors on va s'assurer de faire en sorte que ce soit aussi utile que possible et diffuser autant que possible. Ça y est, Nick, j'ai fini.

NICK WENBAN-SMITH : Merci David, presque dans les temps.

Je vois qu'il y a un commentaire par rapport au lancement du référentiel. Et vous aurez l'occasion d'inscrire plus de questions sur le chat pour David. J'ai une question à lui poser et David, j'en ai déjà parlé, donc c'est une question amicale.

On voit qu'il y a beaucoup de ressources de la communauté, d'énormes ressources qui sont consacrées au référentiel et à la gestion du contenu.

On voit tout l'effort au niveau des ressources qui est déployé. Moi, je parle toujours des ressources et des volontaires qui sont des ressources finies et non pas infinies au sein de cette communauté. Comment avez-vous décidé de la durée de ce travail ? Je me rappelle que TLD Ops a pris pas mal de temps avant d'attirer l'attention et maintenant, cela attire une bonne partie des ressources de la communauté. Mais comment est-ce que vous voyez les choses, vous, pour vous assurer qu'on ne doive pas attendre plusieurs années pour voir le résultat de ce référentiel ?

DAVID MCAULEY : Très bonne question. Je pense qu'on y a réfléchi pas mal, mais d'abord on pense que la meilleure chose à faire, c'est de voir ce qu'en pense la communauté, quelles sont ses réactions, quels sont ses commentaires. C'est pourquoi on vous demande quatre ou cinq questions avec ce sondage et ensuite, lors des prochaines conférences de l'ICANN, on vous renverra des petits rappels pour répondre à ce sondage pour encourager une adoption précoce et pour vous demander en ligne vos retours par rapport à l'utilité du référentiel. Ceci va donc dépendre du DASC dans son ensemble, de savoir à quel point ce mouvement est dynamique et avance et non pas de [nous].

NICK WENBAN-SMITH : Merci. Diapo suivante, s'il vous plaît.

Un petit résumé ici. Il y a deux groupes de travail au sein du DASC et on vient d'entendre le référentiel. Le deuxième, c'est le sous-groupe sondage. Je vais faire un bref récapitulatif de ce qu'on a fait.

Au cours du dernier trimestre 2022, il y a eu un bon taux de réponse avec une bonne répartition géographique et linguistique. C'est une excellente chose. Vous voyez ici les principaux chiffres mais parfois, il faut comprendre ce qu'il y a derrière ces chiffres. On sait que certains gestionnaires de ccTLD ont de nombreux TLD et ne répondent que pour un, mais il faut bien comprendre l'opinion de tout un chacun lorsqu'on répond à un sondage. Diapo suivante, s'il vous plaît.

C'est une diapo assez intéressante qui illustre bien qu'on me donne une livre ou un dollar à chaque fois qu'on me dit que les ccTLD diffèrent les uns des autres, je serais probablement millionnaire maintenant. Mais vous voyez à quel point il y a variété dans le monde des ccTLD. C'est pour cela que lorsque vous regardez les résultats d'un sondage, il y a certaines choses qui sont propres au modèle des registres. Certains registres ccTLD ont des politiques d'enregistrement très restrictives. Je sais que certains au niveau européen ont une obligation de vérifier l'identité pour les titulaires de nom de registre, c'est obligatoire, sur le modèle gTLD. Il faut voir ces données et à ce moment-là, il faut réfléchir par rapport à ce que vous cherchez et à ce qu'il ne faut pas perdre de vue. Diapo suivante s'il vous plaît.

On a regardé ce qui s'est passé lors de l'ICANN76, il y a des enregistrements qui sont disponibles, et on a reçu des questions qui se concentraient surtout sur les mesures proactives pour lutter contre l'utilisation malveillante du DNS. On a eu beaucoup de discussions et de questions par rapport aux méthodes et outils que les ccTLD utilisent. Et en fonction de la définition du mot abus ou utilisation malveillante

du DNS, vous avez beaucoup de faux négatifs dans les retours d'information par rapport aux listes de blocage et de réputation. Donc, il faut absolument partager les informations par rapport à ce que ce qui est bon d'être utilisé par les ccTLD pour faire face à ces faux positifs, justement. Ce serait réellement intéressant de le faire au niveau de la communauté et peut-être que nos efforts combinés pourraient faire un effet boule de neige positif sur les autres et encourager les autres à les utiliser aussi. Également regarder les variations régionales ; il y a énormément de diversité en termes de taille et de modèle de registre, etc. Ce sont des conclusions très intéressantes. Diapo suivante, s'il vous plaît.

Je vais maintenant donner la parole à ma collègue Tatiana.

TATIANA TROPINA : Merci beaucoup. Nous sommes ravis de vous présenter les résultats de notre prochaine partie. Nous allons analyser les données pendant le cycle de vie d'un nom de domaine pour lutter contre l'utilisation malveillante du DNS. Ce sont des données très importantes. On pourrait regarder plusieurs pratiques de façon à connaître l'ensemble du cycle de vie.

Il y a beaucoup de choses ici qui entrent en jeu. Il s'agit d'une enquête, donc on ne peut pas faire de comparaison entre les vérifications faites. Parfois même, on ne peut pas avoir de relations. Mais ce que ces données nous montrent, c'est la richesse des pratiques, des techniques, des outils que les ccTLD utilisent pour maintenir la santé du

DNS et pour lutter de manière proactive contre l'utilisation malveillante. Vous allez voir que les approches sont différentes. Nous encourageons les gestionnaires de ccTLD à présenter ces informations, à partager les meilleures pratiques et à réutiliser ces informations.

Je l'ai dit pendant l'ICANN76, je sais que tout le monde n'était pas là donc je vais le répéter, parfois quand on regarde les statistiques, on le verra tout à l'heure, ce n'est pas toujours très clair. Avant de vous montrer les statistiques, je voudrais dire qu'une des choses les plus intéressantes à analyser lorsqu'on regarde les résultats des enquêtes, c'est que ces enquêtes nous permettent d'avoir des données mais aussi des commentaires des participants. Ceci nous montre qu'il n'y a pas une seule solution qui correspond aux besoins de tous. Cela montre aussi que les pratiques diffèrent, qu'elles sont riches. On peut avoir des choses basées sur « connaissez votre client » ou d'autres types de choses et des combinaisons de ces différentes approches aussi comme vous le voyez ici dans les 24 heures suivant l'enregistrement en cas de réclamation et parfois, c'est tous les mois en cas de réclamation, en cas de plainte, de manière aléatoire, quelle que soit la date d'enregistrement. Vous voyez, il y a une combinaison de vérifications manuelles et automatiques. Les ccTLD partagent cela avec nous, ils invitent des étudiants à regarder les données de manière manuelle aussi et certains ccTLD font des vérifications automatiques mais ensuite vérifient à nouveau lorsqu'il y a des chiffres ou des données d'enregistrement trop élevés. Certains ccTLD nous ont envoyé ces données et nous avons pu faire des relations entre les bureaux

d'enregistrement et les registres. Parfois, certains ont des politiques d'un type, d'autres d'un autre type.

Je vais maintenant donner la parole à ma collègue Angela.

ANGELA MATLAPENG : Merci Tatiana.

Bonjour à tous les participants. Je suis Angela, j'appartiens au ccTLD .bw. Je vais vous montrer des résultats que l'on a obtenus en fonction des données indiquées par Tatiana.

Nous avons devant nous des informations qui sont collectées au niveau de l'enregistrement. Si vous regardez, vous voyez les différences entre les données collectées et les données validées. Vous voyez qu'il y a une marge entre ce qui est collecté et ce qui est validé, et la plupart des ccTLD ou la plupart des répondants indiquent qu'ils n'ont pas pu valider certaines données. Ce qui qu'on a maintenant, c'est le nom du contact, l'adresse e-mail et on voit que certaines informations qui sont collectées lors de l'enregistrement sont de manière générale assez intéressantes et peu nombreuses. Et pas tous les bureaux d'enregistrement collectent ce type de données.

Les différentes approches, on en a parlé, on a parlé aussi d'avoir des contacts rédigés clairement, parfois, on a cet accord avec le bureau d'enregistrement. Mais dans le cas où une utilisation malveillante a lieu au niveau du contenu ou au niveau de codes malveillants qui sont injectés, à ce moment-là, on a besoin d'avoir ce contact pour savoir à

qui appartient ce domaine et pourquoi on a ce type de contenu ou autre problème.

Ici, vous voyez une relation entre le préenregistrement et la rénovation. La plupart des personnes qui ont répondu ont indiqué qu'ils n'avaient pas nécessairement réalisé une vérification et ce type de choses existe, surtout au niveau de la rénovation.

Un des commentaires qu'on a reçus était que certains registres traitent les enregistrements comme un seul enregistrement. Par conséquent, on vérifie les informations la première fois et ensuite cette vérification n'est pas refaite. Du côté droit, vous voyez les différentes manières de faire ces vérifications. Ce que l'on a constaté, comme Tatiana l'a dit, on a des vérifications manuelles, certaines personnes qui ont répondu ont dit qu'ils avaient un système automatisé avec des outils ou qu'ils avaient une combinaison entre manuel et automatisé. Il y a aussi un chiffre élevé de personnes qui ont répondu en disant qu'ils ne faisaient aucune vérification.

Si l'on regarde maintenant ce qui se passe ou le type d'actions que les ccTLD vont avoir après l'enregistrement, on a une indication qu'on ne va pas immédiatement mettre en place des actions comme effacer un domaine immédiatement ou le suspendre en cas de problème. La plupart des registres disent qu'ils vont analyser le risque et voir les résultats en découlant. Bien sûr, on a des bureaux d'enregistrement et des ccTLD qui ne mettent en œuvre aucune action.

Lors de la réunion précédente de l'ICANN, on a présenté des informations comme quoi les ccTLD n'avaient pas les outils corrects pour répondre à ce type de problème. Cela n'a pas été une surprise. Lorsqu'on voit les réponses ici à ces enquêtes, souvent on nous dit qu'on ne met pas en place de réponse parce qu'on ne sait pas très bien que faire.

L'autre question portait sur ce que les ccTLD font lorsqu'ils reçoivent une demande d'agir de la part du gouvernement ou des forces de l'ordre. Ici, c'est différent des questions préalables et on voit qu'ils disent qu'ils font de la diligence due, qu'ils exécutent les demandes sans vérifier davantage.

Pour résumer, les conclusions de cette diapositive seraient que certaines questions concernant les ccTLD, s'ils sont affectés par les législations de protection de données, on constate que même si la plupart des répondants ont dit que oui, on se demande encore si les personnes qui font ces vérifications. Beaucoup ont dit que non, mais beaucoup ont dit aussi qu'en fonction de la législation, ils peuvent agir. On pense que tout ceci est lié à la question liée à l'exactitude des données WHOIS et autres et que cela joue un rôle important.

Je vais maintenant donner la parole à mon collègue Bruce.

BRUCE TONKIN : Merci.

Lorsque nous avons présenté ces résultats, nous avons demandé aux ccTLD quel était le niveau d'utilisation malveillante qu'ils avaient

constaté. On a reçu 57 réponses. La plupart disaient qu'ils avaient moins de 0,05 %. La question ici est : est-ce qu'on peut dire qu'il y a plusieurs catégories qui sont classées ? On est allé à l'institut qui travaillent sur ce thème-là, on a travaillé avec plusieurs organisations qui rapportent des problèmes d'hameçonnage, de botnet, etc. On a regroupé tout cela, on a analysé tout cela en fonction des codes pays et on a essayé d'analyser les réponses.

L'Institut sur l'utilisation malveillante du DNS nous a dit qu'on avait 0,05 % de domaines qui faisaient une utilisation malveillante du DNS. Par conséquent, on pourrait parler d'utilisation malveillante liée à l'utilisation de marques et autres. En tout cas, il faudrait avoir une définition commune entre les ccTLD ; ce serait important puisque tous les ccTLD indiquent que les niveaux d'abus ne sont pas très élevés. Et on sait que les ccTLD peuvent avoir des millions d'enregistrements. Ce serait les résultats de cette enquête. Nous voyons que ce sont des résultats plutôt bas et qu'on a des niveaux d'utilisation malveillante qui correspondraient à des centaines. Par conséquent, si on parle de code de pays, cela correspondrait à des millions. Est-ce qu'il y a des actions qui sont prises dans ce sens, qui sont mis en œuvre pour lutter contre cela ? C'est ce qui reste à voir.

Prochain thème. Nous avons reçu des questions de la part du GAC et de la part des ccTLD concernant la tarification et le niveau d'abus. La première chose que nous avons faite, c'est que nous avons pris les 57 réponses que nous avions reçues, nous nous sommes rendus sur les sites Internet et nous avons analysé les processus pour ces TLD. Vous

voyez que la plupart des ccTLD ici vont demander entre 20 et 100 $; c'est un chiffre assez élevé. Il y a quelques ccTLD qui demandent davantage que cela.

Nous avons regardé les niveaux d'utilisation malveillante et les tarifs et nous avons les comparés. Nous avons constaté que les niveaux étaient les mêmes et qu'il n'y avait pas vraiment de corrélation entre la tarification et le niveau d'utilisation malveillante et que ce n'était pas une tendance claire. Peut-être que c'est plutôt lié non pas à la tarification mais aux outils et aux techniques utilisées par ces ccTLD pour lutter contre ces utilisations malveillantes. Parfois, il y a des systèmes automatiques qui font que l'on peut automatiquement suspendre ou effacer un nom de domaine, tandis que pour un ccTLD qui a un prix plus élevé, il y a des contrôles manuels qui permettent un plus haut niveau de contrôle, donc ils peuvent plus facilement détecter les abus. La conclusion, c'est qu'on n'a pas pu trouver de corrélation entre le prix et le niveau d'abus.

NICK WENBAN-SMITH : Très bien, merci beaucoup.

On a eu deux séances maintenant sur ce sondage : d'abord une séance d'introduction de haut niveau et une autre sur les conclusions et quelques analyses en profondeur sur les données d'enregistrement et la question du prix, de la tarification et c'est une question particulièrement intéressante parce qu'on essaie de maintenir les prix

aussi bas que possible et l'argument selon lequel un prix faible égal un plus haut niveau d'abus ne semble pas probant.

BART BOSWINKE : Il y a une question et un commentaire avant de passer à la question suivante. La question de Raitme Cittera est la suivante : « Est-ce qu'on considère une bonne pratique pour les ccTLD de réunir leurs efforts avec les FSI locaux pour identifier les modèles éventuels en matière d'utilisation malveillante du DNS ? »

NICK WENBAN-SMITH : Non, je pense que non. Mais si vous attendez les prochaines étapes, c'est justement la thématique qu'on va aborder lors des prochains ateliers de travail, je vais souligner cette question.

BART BOSWINKEL : Ensuite, il y a commentaires sur la tarification et un autre commentaire qui arrive. D'abord sur la tarification : « Les ccTLD utilisent une promotion à un dollar et ils ne peuvent pas détecter la corrélation entre le prix et le niveau d'abus. »

BRUCE TONKIN : Ce que j'ai utilisé sur ce graphique, c'est un prix moyen plutôt qu'un prix promotionnel et les TLD, qu'ils soient ccTLD ou gTLD, utilisent des promotions. Mais on n'a pas fait d'évaluation des promotions en général pour voir s'il y avait un plus haut niveau d'abus ou pas.

NICK WENBAN-SMITH : C'est un commentaire intéressant et peut-être qu'il faudrait être prudent et ne pas tirer de conclusions trop hâtives du lien avec le prix au détail parce qu'on sait que les opérateurs de registre et les bureaux d'enregistrement vendent en dessous du prix au bureau d'enregistrement parce qu'ils font leurs marges non pas sur un domaine mais sur une autre activité. Donc, ils retirent les marges sur les autres services qu'ils offrent.

Peut-être qu'au niveau des opérateurs de registre, ce peut être le cas, mais s'il y a une promotion spécifique et une campagne à un dollar, il faut être prudent et ne pas se précipiter sur une conclusion.

Du point de vue des ccTLD, je ne sais pas si on peut faire grand-chose par rapport au prix qu'offrent les bureaux d'enregistrement. S'ils veulent une bonne promotion, on pourrait rentrer sur un terrain dangereux et pas approprié. Mais oui, commentaire intéressant.

Maintenant, il y a un autre commentaire de John McCormack par rapport à l'utilisation malveillante de ccTLD qui est souvent une tendance pour l'hameçonnage des sites compromis.

BART BOSWINKE : Nick, nous avons une main levée de Mike Chattan.

MICHAEL CHATTAN : Je sais qu'il y a aussi des programmes de croissance qui sont proposés et je ne sais pas si c'est une bonne chose ou une mauvaise chose si on peut le dire.

NICK WENBAN-SMITH : Je pense qu'on est tous d'accord pour dire que s'il y avait moins d'enregistrements, le nombre d'abus serait plus faible. Mais c'est une tendance entre fournir une ressource utile à l'industrie que les PME peuvent utiliser aussi massivement que possible et atténuer cette utilisation malveillante, d'où tout l'intérêt de cette question.

On a pas mal de travail en cours, comme vous venez de l'entendre, au niveau du référentiel qui est en train de travailler sur sa liste de diffusion, qui est en train de l'étendre. On attend le lancement formel de cette liste de diffusion.

Maintenant, du côté du sondage, je pense que le sous-groupe sondage a trouvé un exercice très intéressant à faire et nous aimerions organiser un autre sondage tout en sachant qu'il ne faut pas dépendre trop non plus de la communauté et de ces réponses au sondage. Ce que je propose, c'est qu'on fasse un autre sondage, peut-être au dernier trimestre de 2024, mais on ne veut pas le faire si la communauté pense que c'est embêtant et que ce n'est pas utile.

On vous pose une question dans le cadre du sondage : est-ce que vous voulez un autre sondage ? Est-ce que vous pensez que les résultats d'un autre sondage seront intéressants ? Sur l'écran, ça dit novembre 2025, mais je pensais à 2024. Écoutez, c'est novembre 2025… non, on me dit

2024. J'essaie de lire et de parler en même temps, ce n'est pas simple. Très bien, 80 %.

On va regarder certaines questions du sondage où on a vu certaines incohérences dans les réponses pour voir si on pourrait peut-être poser des questions plus claires pour la suite. On va essayer de poser des questions qu'on n'a pas encore posées. L'idée serait d'avoir les principales questions identiques à celles-ci pour ne pas trop essayer d'extrapoler par rapport aux résultats et voir si cette initiative, non seulement au sein de la ccNSO mais au sein de toute la communauté, est en train de parvenir à quelque chose en termes d'utilisation malveillante du DNS.

Il y a une autre question ici. Est-ce que vous voulez une analyse encore plus approfondie par rapport à ce sondage pour l'année calendaire ? Écoutez, je ne sais pas si dans le public ce sont des personnes particulièrement mordues de cette thématique. Je suppose qu'il y a un échantillon bien particulier dans la salle, c'est pourquoi on obtient ces réponses. Mais on va en prendre bonne note, merci.

J'insiste sur le fait que c'est censé être un processus à double sens, c'est-à-dire qu'on a vraiment besoin de vos retours. Mais il semblerait qu'il y ait un souhait de continuer à explorer ces questions si intéressantes et les liens qui existent entre toutes ces thématiques.

On a quelques questions ici. Bart, est-ce que vous pouvez m'aider à analyser les questions et commentaires ? Parce qu'il y en a beaucoup.

BART BOSWINKEL : Questions par rapport au travail en cours. Mais on a encore quelques questions. Est-ce qu'on peut revenir en arrière, s'il vous plaît ? « Quels sont les prochains jalons dans le travail du DASC puisqu'on a le référentiel et la liste de diffusion ? »

NICK WENBAN-SMITH : Lorsque je présentais les premières données, il y a eu beaucoup de questions par rapport ont fait que oui, tout ceci est bien intéressant, mais pourquoi est-ce que vous n'étudiez pas une thématique en particulier ? Et je dois vous dire que j'ai appliqué quelques jugements purement subjectifs par rapport aux questions et commentaires que j'ai reçus par rapport à ces quatre thématiques.

On a quatre suggestions à l'écran. S'il y en a d'autres, surtout, n'hésitez pas à nous les soumettre pour considération. Mais il y a quatre domaines qui sont apparus comme étant nécessaire à approfondir ou faire l'objet d'un atelier prochain. Je reviens au mandat du comité permanent, à savoir partager les meilleures pratiques, éduquer et fournir des ressources à la communauté.

Tout d'abord, on a déjà analysé cela parce que c'est quelque chose d'assez évident par rapport aux enregistrements, aux politiques, au niveau d'utilisation malveillante ; on pourrait donc avoir un examen plus approfondi autour de cette question. Ceci a été la première question et je suppose que beaucoup de gens le savent déjà, mais si ce n'est pas le cas, en tant que ccTLD, il faut être très prudent par rapport à toutes les questions liées au contenu. Mais la gestion du contenu par

l'intermédiaire des plaintes, ceci revient très souvent à dire : « On n'a pas de politique en termes de plaintes. » Et si vous êtes confronté à une menace ou à quelque chose de malveillant, faites-le-nous savoir. Ceci passe plus par l'analyse de la qualité de données.

La deuxième thématique a à voir avec la question autour des tarifications, des prix et des promotions. Le fait est que le mécanisme de marketing et la relation avec le client, à savoir les bureaux d'enregistrement, font qu'il faudrait peut-être être plus intelligents dans notre relation avec les bureaux d'enregistrement pour lutter contre l'utilisation malveillante du DNS. Le lien entre opérateurs de registres et bureaux d'enregistrement et cette relation peuvent être très utiles pour lutter contre l'utilisation malveillante du DNS. C'est la deuxième thématique.

Pour la troisième thématique, d'après le premier sondage, on voit qu'il y a un peu plus de 30 % des répondants qui ne sont pas sûrs par rapport aux résultats et au niveau d'abus dans leur propre ccTLD. Peut-être que c'est parce qu'ils ne le savent pas et que c'est simplement un petit ccTLD, et un petit ccTLD n'a pas les moyens d'assurer un suivi et d'avoir des chiffres clairs. Donc, outils de référence et mesures pour assurer un suivi. Il y a également le projet DAAR de l'ICANN qu'on peut regarder pour s'inspirer puisqu'il y a des outils et des mesures qui existent et ceci pourrait nous éclairer un petit peu par rapport à certaines questions sur lesquelles on avait du mal à avancer, qu'on avait du mal à comprendre pour pouvoir faire des comparaisons et voir ce qui a marché pour la

communauté, ce qui n'a pas marché. Ceci pourrait être quelque chose de très utile pour travailler à ce niveau-là.

La quatrième thématique. C'est facile de ralentir un petit peu le rythme lorsque vous ne vous sentez pas emporté par la thématique puisqu'il s'agit de gouvernance. Au sein de la ccNSO au fil des ans, on a eu plusieurs modèles de gouvernance, mais il me semble qu'on ne s'est jamais penché sur l'intersection entre les cadres juridiques et les modèles de gouvernance et vu lequel des deux réussit mieux au niveau de l'atténuation de l'utilisation malveillante du DNS. Ce serait la quatrième thématique.

Nous pouvons maintenant passer à la prochaine question de notre enquête : dites-nous si les thèmes de travail vous intéressent ? En termes de priorisation, est-ce qu'il y aurait un thème qui vous paraîtraient à prioriser ? Est-ce que vous voulez nous l'indiquer ? Avec cette question, nous essayons de prioriser un ou deux thèmes de façon à aborder ces questions en premier lieu. Si vous voulez répondre, dites-nous seulement quels sont les thèmes que vous voulez analyser en premier lieu. Mettez une marque en face du thème de votre intérêt : outils et mesures, validation des données et politique de préenregistrment, en collaboration avec les bureaux d'enregistrement, impacts et modèles gouvernementaux sur le niveau d'utilisation malveillante du DNS et pas intéressé. Voilà les réponses. Je pense que nous recevons ce que nous méritons comme réponse.

Outils et mesures est la réponse qui a été la plus choisie ; ceci va nous permettre de choisir nous-mêmes les outils et les des choses qu'on veut

aborder. Je vais essayer d'aborder un de ces thèmes lors de la réunion de Hambourg. Nous allons en parler avec le comité permanent et essayer de parvenir à un accord. Je pense que c'est une grande tentation de se centrer sur ce que nous faisons avec les ccTLD. Mon objectif est un travail plus intercommunautaire avec les bureaux d'enregistrement, l'ICANN, les équipes techniques, le personnel, les équipes qui travaillent sur les mesures et avec les différentes parties contractantes. Il y a des choses très intéressantes qui sont faites actuellement à ce niveau-là. Ce serait intéressant comme collaboration.

BRUNCE TONKIN : Une des choses intéressantes ici serait la différence entre les noms de domaine et les enregistrements. Parfois, certains noms de domaine sont enregistrés exprès pour une action malveillante par une organisation sur un site Internet ; parfois, un site Internet a été détourné et utilisé dans ce sens. Dans la première catégorie ici, la validation des données et les politiques d'enregistrement pour les ccTLD, il y a des questions qui sont importantes.

NICK WENBAN-SMITH : Bonne observation. On a analysé les questions liées aux ccTLD et aux utilisations malveillantes. Beaucoup de ccTLD qui sont là qui travaillent avec nous depuis plus de 30 ans ont une tendance à une certaine maturité. Nous sommes dans cette étape de maturité ; par conséquent, la quantité d'abus pour des ccTLD murs va être plus focalisée sur les

domaines détournés que sur d'autres. Je crois que c'est un domaine très intéressant et je sais que dans certains registres, nous avons mis en place des actions contre des titulaires de nom de domaine qui étaient innocents mais leur nom de domaine était suspendu quand même. Ce n'est pas quelque chose de très courant mais ceci arrive et c'est arrivé au .uk. Parfois, les validations de données vont lutter contre des utilisations malveillantes. Ce n'est pas toujours que le titulaire de nom de domaine est responsable de cette situation. Très souvent, c'est simplement une victime de cela. Il n'est pas coupable.

Je vais voir un petit peu les commentaires et les questions. Il y a une personne qui lève la main. On lui donne la parole.

MAHUM KHAWAJA : Bonjour, je suis Mahum, j'appartiens au groupe NextGen et je suis du Canada. Je voulais poser une question sur le référentiel. C'est une précision concernant le référentiel. Quelle est la différence entre le référentiel et le Wiki de l'ICANN puisqu'il s'agit d'une base de données ?

NWB : Très bien, bonne question. Merci et bienvenue. David, allez-y.

DAVID MCAULEY : Quelle est la différence par rapport au Wiki de l'ICANN ? Merci, c'est une bonne question. Le référentiel que nous avons mis en place va se centrer sur des informations utiles aux gestionnaires de ccTLD parce que très souvent, ceci pourra être utile à d'autres aussi. Mais nous allons

d'abord nous centrer sur cette communauté en particulier et essayer d'être un peu plus centrés sur les informations de ce type plus que ce que le Wiki pourrait faire. De toute façon, c'est vrai que ce sera probablement assez proche du Wiki de l'ICANN. Merci.

NICK WENBAN-SMITH : Est-ce qu'il y a d'autres questions dans la salle ou sur Zoom ?

BART BOSWINKEL : Nick, il y a une question qui porte sur les fournisseurs de service Internet : « Est-ce que c'est une bonne pratique de travailler avec les ISP locaux pour identifier des utilisations malveillantes du DNS pour les ccTLD ? »

NICK WENBAN-SMITH : Oui, c'est une bonne question. Je pense que lorsque l'on veut parler des actions que l'on peut faire avec les bureaux d'enregistrement en collaborant avec eux, on peut parler du fait que la collaboration se fait non seulement avec les bureaux d'enregistrement mais avec les juridictions et ceux qui sont responsables en général de la fourniture de l'Internet, à savoir les ISP. C'est un domaine intéressant. Personnellement, je ne connais pas énormément de ccTLD qui travaillent en collaboration étroite avec les ISP, mais je sais que certains bureaux d'enregistrement le font. On tente de travailler en collaboration entre l'ISP et le bureau d'enregistrement.

BRUCE TONKIN : Une observation que j'ai dans le domaine des ISP est qu'ils utilisent les données concernant les flux d'utilisation malveillante du DNS, ils les partagent, ils les diffusent et ils les bloquent sur leur site Internet. Lorsque les contenus de logiciels malveillants sont retirés, on constate que l'ISP les a bloqués.

NICK WENBAN-SMITH : Je voudrais être un peu plus prudent sur cette question. Je ne veux pas critiquer les fournisseurs qui bloquent ces listes. Je sais que c'est parfois plus facile de retirer quelque chose qui a été détourné, mais on constate que ça reste ensuite pendant des années, voire des dizaines d'années. Même si le nom de domaine a été annulé, cela reste parfois ce que l'on appelle des faux positifs. Un haut degré de prudence est nécessaire ici parce qu'on voit qu'on essaie d'utiliser des systèmes automatiques, mais on doit encore faire certains processus de manière manuelle pour éviter des erreurs. C'est un point intéressant ici à souligner.

Il ne nous reste plus que trois minutes. Je veux remercier tous les intervenants, tous ceux qui ont posé des questions aussi. S'il n'y a pas d'autres questions, je vous remercie beaucoup pour votre participation et nous attendons votre contribution pour savoir dans quel secteur vous voulez que l'on commence à travailler.

J'ai déjà présenté cela lors de la réunion de Cancún, ce qui me permet d'avoir déjà la contribution de la communauté. Et dans quelque temps,

après le lancement du référentiel, nous aurons davantage de données pour mieux connaître vos opinions.

Je vous remercie. Je remercie mes collègues copanélistes qui m'ont accompagné ici. Cela a été un véritable plaisir et je les remercie.

ORATEUR NON-IDENTIFIÉ : Nous allons stopper l'enregistrement. Merci.

[FIN DE LA TRANSCRIPTION]