ICANN78 | Réunion générale annuelle – Discussion du GAC sur l’utilisation malveillante du DNS
Mercredi 25 octobre 2023 – 10h30 à 12h00 HAM

GULTEN TEPE : Bonjour et bienvenue à la discussion du GAC de l'ICANN78 sur l'utilisation malveillante du DNS en ce mercredi 25 octobre à 8 h 30 UTC. Je m'appelle Gulten et je suis responsable de la participation à distance pour cette séance. Veuillez noter que la séance sera enregistrée et sera régie par les normes attendues du comportement de l'ICANN

Pendant cette séance, les questions et les commentaires envoyés dans le chat ne seront lus à voix haute que s'ils sont formulés correctement. L'interprétation pour cette séance inclura les six langues des Nations Unies et le portugais. Veuillez cliquer sur l'icône d'interprétation dans Zoom et sélectionnez la langue dans laquelle vous allez écouter la séance. Si vous souhaitez parler, levez la main dans la salle Zoom et une fois que le modérateur aura appelé votre nom, mettez en marche votre micro et prenez la parole.

Avant de parler, n'oubliez pas de sélectionner la langue que vous parlerez dans le menu d'interprétation. Veuillez donner votre nom pour l'enregistrement et la langue dans laquelle vous allez parler, si c'est une langue autre que l'anglais. Lorsque vous parlerez, n'oubliez pas d'éteindre les autres dispositifs et notifications. Parlez clairement et lentement pour permettre une bonne interprétation de vos propos.

Pour lire la transcription en temps réel, vous pouvez cliquer sur le bouton Closed Caption dans le menu de Zoom. Pour assurer la transparence de la participation au modèle multipartite de l'ICANN, nous vous demandons de vous inscrire dans les séances de Zoom en utilisant votre nom. Ceci étant, je vais céder la parole au président du GAC, Nicolas Caballero.

NICOLAS CABALLERO : Merci beaucoup, Gulten. Bienvenue à tous. Nous allons avoir une séance de 90 minutes très intéressante sur l'utilisation malveillante du DNS, un sujet très sensible et très important pour nos collègues distingués qui sont présents ici à Hambourg. Nous avons une équipe fantastique d'intervenants, mais je vais les laisser se présenter en commençant par mon ami Graeme.

GRAEME BUNTON : Bonjour à tous, je m’appelle Graeme. Je suis directeur exécutif du DNS Abuse Institute.

LAUREEN KAPIN : Bonjour à tous, Je m'appelle Laureen Kapin et je parlerai en mon propre nom ainsi qu'au nom du groupe de travail sur la sécurité publique dont je suis co-présidente.

NICK WENBAN-SMITH : Bonjour à tous. Je suis Nick Wenban-Smith. Je suis juriste au Royaume-Uni mais je vais parler en tant que président du comité de la ccNSO.

SUSAN CHALMERS : Bonjour à tous, Je m'appelle Susan Chalmers et je travaille pour l'administration, la NTIA au département du commerce des Etats-Unis. Je suis ici en tant que représentante au GAC de mon pays.

CHRIS LEWES-EVANS : Bonjour à tous. Je m'appelle Chris Lewes-Evans. Je suis directeur de la relation avec les parties prenantes et je m'occupe du clean DNS.

SAMANEH TAJALIZADEHKHOOB : Bonjour à tous. Je m'appelle Samaneh et je suis responsable du groupe SSR au sein de l’ICANN Org pour le bureau de la technologie.

NICHOLAS CABALLERO : Très bien, merci beaucoup. Je vais immédiatement céder la parole à Laureen qui va nous présenter… Pardon, c'est Susan qui va s'occuper de cette partie. Susan, allez-y.

SUSAN CHALMERS : Merci d'être avec nous aujourd'hui. Nous avons un ordre du jour bien rempli pour cette séance, donc je vais brièvement vous donner le contexte des amendements aux contrats pour utilisation malveillante du DNS. Donc, c'est un sujet ouvert par les parties prenantes. Et donc je vais parler du processus de consultation publique et de la contribution du GAC relatives à ces amendements au contrat.

Diapositive suivante, s'il vous plaît! Merci. Aux environs de 2019, le GAC a commencé à se concentrer sur cette question de l'utilisation malveillante du DNS, ainsi que d'autres parties de la communauté de l'ICANN, en demandant davantage d'actions au sein du travail de l'ICANN. Les parties contractantes ont répondu avec une proposition proactive pour traiter de ces questions d'utilisation malveillante du DNS. Fin 2022, il y a eu une proposition de négocier de nouvelles obligations en matière d'utilisation malveillante du DNS dans les deux contrats. Les noms de ces contrats sont à l'écran pour ceux qui ne les connaissent pas.

En mai 2023, les propositions d'amendements ont été publiées et le processus de consultation publique a démarré en juillet 2023. Le GAC a envoyé un commentaire public et nous allons en parler à la diapositive suivante. J'aimerais noter que, en octobre, la période de vote pour l'adoption de ces amendements a commencé et elle devrait se conclure en décembre. Diapositive suivante, s'il vous plaît.

Avant l'ICANN77, certains membres du GAC se souviennent peut-être que nous avons travaillé avec un groupe de travail des régions faiblement desservies et nous avons donc proposé deux webinaires pour donner davantage de contexte à l'utilisation malveillante du DNS et pour expliquer l'objectif des amendements. J'encourage tous ceux qui s'y intéressent à regarder ces webinaires et vous les avez sur le site du GAC. Ensuite, à l'ICANN77, nous avons organisé un atelier de renforcement des capacités, également mené par le groupe de travail sur les régions faiblement desservies avec les Etats-Unis. Nous avons travaillé avec notre groupe de travail pour produire cet atelier. Nous

avons parlé des amendements aux contrats, mais aussi, de manière peut être plus importante, du commentaire public que devait publier le GAC pour l'envoyer au processus de consultation publique.

Nous avons eu la chance d'avoir des volontaires qui ont proposé de participer. Les délais étaient assez courts – les délais de cette consultation publique donc. Les représentants étaient de Taipei, de Chine, de Colombie, d'Égypte, de la Commission européenne, du Royaume-Uni et des Etats-Unis, du Mali et de la Suisse. Nous avons consulté toute la liste des membres du GAC et le commentaire public a également été informé par le travail du Groupe de travail sur la sécurité publique.

La période de commentaires publics a été en faveur largement de ces amendements et ce que je peux vous dire avec mes collègues, c'est que nous devrions encourager les opérateurs de registre et les bureaux d'enregistrement à voter en faveur de l'adoption de ces amendements. Donc, veuillez y réfléchir. Les commentaires publics ont quand même identifié des domaines de travail pour l'avenir et pour ceci, je vais céder la parole à ma collègue Laureen de la Commission fédérale des échanges.

LAUREEN KAPIN : Merci Suzanne. Donc ce que je peux vous dire, c'est qu'une fois que ces amendements seront approuvés, il y aura encore du travail. D'ailleurs, nous en avons parlé dans le cadre du commentaire public du GAC à ce sujet. Un des domaines dont nous avons parlé, c'était donc des processus d'élaboration de politiques ciblées pour informer les

contrats et le travail. Dans ce domaine, on dit ciblé. Ciblé, qu'est-ce que ça veut dire? Ça veut dire qu'il faut que la focalisation soit étroite, précise et donc nous espérons rapide.

Donc voilà certaines des choses que nous avons identifiées dans les commentaires. Alors je vous dis ceci pour rappel et pour aussi motiver peut-être certaines réflexions. Donc les termes clés dans les amendements, il y a des termes clés, c'est approprié, prompte, exploitable et raisonnable. Donc c'est le type de réponse, les types de réaction plutôt qui doit être entreprise en cas d'abus. On pourrait peut-être mettre en place des indicateurs, des éléments de données qui rassembleront des preuves exploitables. Quelles sont les actions, les mesures d'atténuation qui pourront répondre à certains cas d'utilisation malveillante du DNS?

Autre problème pour faire écho à un des termes. Un problème persistant existe. Comment procéder lorsqu'il y a des récidivistes, lorsqu'il y a en fait une utilisation malveillante persistante? Comment s'attaquer à ce type de problème? L'équipe CCT et l'équipe de révision SSR2 ont beaucoup réfléchi et ont beaucoup d'idées là-dessus. Leur travail a été informé par différentes parties prenantes. Donc il est intéressant de regarder un petit peu ce qui se passe dans ce domaine des réactions, des interventions.

Puis, quelles sont les incitations que l'on peut créer pour les bureaux d'enregistrement qui pourraient donc mener à des résultats positifs. Cela peut être des motivations, donc financières ou autres. Il y a également les questions de diligence raisonnable. Si les titulaires de noms de domaine ont le sentiment d'avoir été suspendu sans

justification appropriée, quels sont les processus qui devraient être mis en place pour remettre en question cette décision? Et enfin, la formation. Il est toujours bon d'avoir des formations sur la prévention et l'atténuation des abus du DNS, de manière à ce qu'à l'avenir on peut promouvoir un bon comportement dans l'écosystème et assurer la sécurité de l'espace.

Diapositive suivante. Il y a des domaines où des travaux devront être faits à l'avenir. Ceci devrait être fait avant la prochaine série, nous l'espérons. Premièrement, la conséquence. La proposition d'amendement inclut des responsabilités, mais ne nous dit pas ce qui se passera si ces responsabilités contractuelles ne sont pas respectées. Donc, à la Conformité de l'ICANN, c'est le travail de cette entité. Mais il serait bon de réfléchir aux conséquences, aux obligations dans le cadre de ces nouveaux amendements s'ils ne sont pas respectés. La possibilité de surveiller est également une question clé. Il serait très utile de pouvoir être transparent par rapport aux résultats que l'on peut observer en ce qui concerne ces amendements précis, et c'est quelque chose qui pourrait faire l'objet d'un travail futur.

Enfin, l'évolution de l'utilisation malveillante du DNS. Nos collègues du SSAC ont rédigé des informations à cet effet dans leur document SSAC515. Vous savez, les mauvais acteurs ont toujours de bonnes combines pour contourner les restrictions. Ils sont très créatifs et donc nous devons faire la même chose. Il n'y a pas de définition qui doit être statique. Donc ceci pourrait donner lieu à une révision par les différentes parties de la communauté, la cybersécurité, les académiques, les chercheurs indépendants, etc., ainsi que les forces de

l'ordre. Ce serait vraiment un domaine qui pourrait donner lieu à des travaux à l'avenir.

Et nous notons que l'avis qui a été publié par rapport aux amendements au contrat devrait être un document vivant, à compléter régulièrement. Donc ce document devrait évoluer de manière à toujours être à jour. Donc voilà un petit peu les sujets qui ont été identifiés dans le cadre des commentaires du GAC et qui devraient nous inspirer pour notre travail à l'avenir dans ce domaine. En tout cas, c'est ce que nous souhaitons.

SUSAN CHALMERS : Diapositive suivante. Merci beaucoup, Laureen. Nous souhaiterions maintenant vous céder la parole pour une discussion d'environ dix minutes et, ensuite, nous passerons aux présentations de nos invités et nous continuerons la discussion plus tard avant de conclure. Donc si vous voulez intervenir et réagir, nous donner vos commentaires, vos perspectives, n'hésitez pas.

GULTEN TEPE : Nous avons plusieurs personnes qui souhaitent intervenir.

NICHOLAS CABALLERO : Oui, j'ai l'Inde, la Chine et le Japon. Commençons par l'Inde.

SUSHIL PAL : Merci beaucoup, monsieur le Président. Encore une fois, c'est une question d'un nouveau venu. Ces problèmes d'utilisation malveillantes du DNS sont quotidiens je crois. Et ce qui m'intrigue, c'est le travail

futur, cette question du travail futur. Est-ce que ce n'est pas plutôt une question urgente qui devrait être traitée dès maintenant?

SUSAN CHALMERS : Merci pour cette intervention. C'est un sujet dont nous débattons depuis longtemps et qui est en cours au sein du GAC. Nous avons eu une séance sur l'utilisation malveillante du DNS à toutes les réunions de l'ICANN ces dernières années.

SUSHIL PAL : Oui, mais vous avez des points qui sont donc à l'ordre du jour pour l'avenir. Ce sont des activités préliminaires qu'on devrait engager pour vérifier les problèmes d'utilisation malveillants du DNS. Mais on ne peut rien faire respecter puisque les amendements ne sont pas encore approuvés. Il y a beaucoup de problèmes qui existent et en fait, on a les mains liées. Il y a des domaines qui appartiennent à nos pays. D'accord, ça va, mais pour ceux qui sont à l'extérieur, on ne peut rien faire.

Donc les amendements contractuels devraient être adoptés très rapidement. C'est une priorité selon moi. Je suis sûr que la communauté en parle déjà depuis un certain temps, mais je crois que c'est vraiment la première chose dont on devrait parler. On devrait agir aussi rapidement que possible parce que nos initiatives ne vont pas aussi vite que celles des cyber-attaquants. Ils piratent ici et là, ils utilisent les algorithmes. Et quels sont les mécanismes qu'on a à notre disposition pour surveiller tout ceci? Comment les condamner?

SUSAN CHALMERS : Oui, je suis entièrement d'accord avec vous. C'est une question absolument prioritaire. Voilà pourquoi il est important d'encourager les bureaux d'enregistrement dans les différentes juridictions de voter en faveur des amendements. Et à San Juan, je pense que nous aurons l'opportunité d'en parler plus – de ces sujets spécifiques que vous avez mentionnés.

NICHOLAS CABALLERO : Merci, Susan, et merci à l'Inde. Alors maintenant, je voudrais m'exprimer en mon propre nom, pas en tant que président du GAC pour dire que je suis absolument d'accord avec vous. Alors, j'ai la Chine. La Chine, allez-y.

WANG LANG : Merci, monsieur le Président. Wang Yang de la Chine. L'ICANN a ouvert cette période de vote pour les propositions d'amendements. Il y a deux seuils à atteindre pour les RAA, approbation du RAA pour les bureaux d'enregistrement et il faut que ce soit 90 % du total pour les domaines sous-gestion. Et pour les contrats des opérateurs de registre dont les paiements à l'ICANN comptent les deux tiers des frais qui ont été payés au cours des années passées. Donc ma question, c'est : Quel a été le niveau d'atteinte de ces seuils récemment et est-ce qu'on peut être optimiste par rapport aux résultats à venir?

SUSAN CHALMERS : Je crois qu'il y a un lien pour faire le suivi qui est fourni par l'ICANN, de manière à ce que nous puissions observer pratiquement en temps réel

ce qui se passe. On peut essayer de voir si on pourrait avoir accès au lien. Donc Fabien va le mettre dans le chat. Vous pouvez donc suivre le progrès.

NICHOLAS CABALLERO : Merci Suzanne. Donc vous pouvez regarder dans le chat, la Chine. J'ai maintenant le Japon.

NISHIGATA NOBUHISA : Le Japon au micro. Alors tout d'abord, merci pour cette excellente présentation et merci pour tout votre travail jusqu'à maintenant. Pour ceux qui sont impliqués dans ce travail, j'ai quelques questions et un commentaire. Première question par rapport aux termes clés que Laureen a mentionné dans la présentation.

Donc nous avons approprié, prompte, exploitable, raisonnable. Ce sont les termes qui ont été utilisés, par exemple dans le RAA 3.18. Donc, est ce qu'on pourrait avoir une directive là-dessus? Si on avait cette directive, est-ce que ceci s'appliquerait aux textes existants par rapport à ces mêmes mots?

Deuxième question par rapport à l'évolution du DNS, donc à la fin de la présentation. Je me demande si certains de nos collègues n'auraient pas des idées sur le type d'utilisation malveillante du DNS qui sera inclus dans la discussion future. On pourrait peut-être réfléchir à un élargissement de ce qu'on utilise comme définition actuelle de l'utilisation malveillante du DNS dans le 515.

Et un autre commentaire par rapport à ce qu'a dit mon collègue de l'Inde, j'aimerais y faire écho. Je partage son opinion lorsque je considère au Japon l'utilisation malveillante du DNS et puis aussi toutes les conduites malveillantes sur l'Internet. Nous devons avoir un

lien, établir un lien entre le GAC et ceux qui contrôlent le ccTLD. Je ne sais pas si je peux parler de la ccNSO et de ce qu'elle fait – Nick peut en parler, mais je crois que c'est plus le fait qu'il y a des questions qui sont communes aux différents gouvernements et donc je pense qu'on pourrait avoir des discussions là-dessus à l'avenir.

SUSAN CHALMERS : Je vais répondre très brièvement à la première question qui a été posée, et ensuite je vais passer la parole à mes collègues pour la deuxième question. Pour ce qui est de la première question, ces termes figuraient également dans le rapport qui a accompagné les amendements. Je vous encourage à lire ce rapport consultatif. Mais il y a également des questions qui restent ouvertes et qui méritent une discussion plus approfondie au sein de la communauté.

LAUREEN KAPIN : Pour rebondir sur ce que Susan vient de dire, s'il y a des PDP ciblés dans cette action, je pense que ce serait un processus d'élaboration de politiques de décider comment cela serait appliqué dans les contrats. Si ce sont les mêmes termes qui seront utilisés, alors on pourrait appliquer ces mêmes termes dans tout le contrat si la communauté décide de le faire. Je veux dire qu'il y a une certaine souplesse par rapport à ces termes et que cela va dépendre des futurs PDP.

Ensuite, il y a un autre aspect. C'est que tout cela doit être fait à l'intérieur et à l'extérieur de l'ICANN. Quand j'écoute nos collègues de l'Inde ou du Japon qui nous font part de leurs difficultés, lorsqu'il y a un comportement malveillant qui vient d'un pays qui s'applique sur un

autre pays, il y a des questions transfrontalières qui se posent et cela implique des négociations, des partages d'informations, des accords de partage d'informations, des accords de coopération. Et tout ce travail se fait en dehors de l'ICANN. Mais c'est un travail extrêmement important pour aider les forces de l'ordre et les autorités de protection des consommateurs du monde entier de travailler ensemble pour essayer de répondre à ce type d'utilisation malveillante. Je voulais souligner cela également.

NICHOLAS CABALLERO : Merci Loreen. Le Japon, est ce que c'est une ancienne main ou vous souhaitez reprendre la parole? J'ai la Colombie. La Colombie est dans la salle.

THIAGO DEL-TOE : Oui, c'est la Colombie. Non. J'ai baissé ma main parce que c'était la même question que la Chine.

NICHOLAS CABALLERO : J'ai la Commission européenne et puis le Canada.

PEARSE O’DONOHUE : La Commission européenne, représentant de la Commission européenne pour les enregistrements. Quand on considère la manière dont nous allons aborder le travail à faire, j'aimerais dire que la Commission européenne soutient les amendements contractuels et ce

travail qui a été fait – nous espérons que ce vote sera positif, je pense que c'est un progrès important.

Cependant, nous devons penser au travail qui reste à faire. Il faut se souvenir qu'il y a une consultation publique et qu'il n'y a pas eu de propositions faites par rapport à ce qui a été soumis à consultation publique. Et donc cela reflète qu'en dehors du modèle multipartite, il y a donc des contrats qui sont passés entre l'organisation ICANN et les parties contractantes, et ils sont à la base du fonctionnement d'une partie clé de l'ICANN et de l'IANA. Je pense qu'il faut voir qu'il y a le besoin de faire en sorte que les parties prenantes du modèle multipartite puissent avoir une influence dans la rédaction des contrats, mais aussi pour qu'ils puissent avoir leur mot à dire par rapport à la mise en œuvre de ces contrats. Les membres du GAC ont déjà évoqué les problèmes que peut susciter l'utilisation malveillante du DNS.

Lorsqu'il faut parler de la surveillance proactive, il faut réfléchir à ce que le PDP puisse être suffisamment détaillé pour pouvoir tenir compte de tous ces problèmes.

NICHOLAS CABALLERO : Le Canada.

JASON MERRITT : Merci beaucoup. Jason Merritt pour les enregistrements. Je voulais profiter de cette occasion avant d'avancer et de passer à un autre sujet, d'exprimer le soutien complet du Canada aux amendements

contractuels. Nous apprécions le travail qui a été fait par l'ICANN, par les parties contractantes, les négociations pour aboutir à quelque chose qui puisse être exploitable, qui puisse être concret et qui constitue une avancée. Je pense qu'il est très positif de penser de manière proactive à d'autres opportunités.

Mais de mon point de vue, nous reconnaissons tous l'effort qui a été investi dans cette initiative et nous savons qu'il faut être attentif. Excusez-moi. On va excuser la personne qui a toussé en fait.

Je voulais faire passer ce message. Nous avons toujours soutenu cette initiative. Nous savons que c'est un effort qui était important pour les parties contractantes également, et c'est un pas énorme qui a été fait. Nous sommes tout à fait conscients de l'effort que cela a demandé.

NICHOLAS CABALLERO : Merci. J'ai l'Iran.

KAVOUSS ARASTEH : Bonjour à tous. Merci beaucoup. Corrigez-moi si je me trompe. L'année dernière, il y a eu des amendements. Est-ce qu'il y en a eu d'autres? Vous savez quelle est la portée de ces autres amendements par rapport aux amendements précédents? Est-ce que l'ICANN pourrait fournir des informations par rapport à la portée des amendements de l'année dernière et la portée des amendements de cette année? Merci.

SUSAN CHALMERS : Je vais être très brève. Merci, Kavouss. Pour ce qui est de l'abus du DNS, il s'agit de la première initiative qui a abouti à des amendements contractuels. Je pense que les amendements précédents concernaient le RDAP, si je ne m'abuse, mais pour ce qui est des amendements dont on parlait ici, c'est la première fois que ces amendements voient le jour en matière d'abus de DNS.

LAUREEN KAPIN : Très brièvement, Kavouss, car il y a eu des documents d'information qui ont été distribués. L'Organisation ICANN, également sur son site web, propose des informations très complètes par rapport à ces amendements, et ces amendements font l'objet d'un vote. Ils n'ont pas encore été… Ils ne sont pas encore en vigueur et nous suivons de très près ce vote pour voir s'ils pourront être approuvés pour le mois de décembre. Voilà où nous en sommes du point de vue de la procédure.

NICHOLAS CABALLERO : Merci beaucoup, Laureen, Susan et l'Iran. Est-ce qu'il y a d'autres questions avant de passer au point suivant de l'ordre du jour dans la salle ou en ligne? Je vois qu'il n'y en a pas. Excusez-moi. L'Indonésie, s'il vous plaît.

ASHWIN SASTROSUBROTO : Je voudrais savoir. Nous savons maintenant ce que les bureaux d'enregistrement doivent faire en cas d'abus du DNS. Il y a une espèce de système de certification pour les bureaux d'enregistrement. Il y a des procédures, par exemple, qui doivent être suivies à l'IUT pour faire

certaines choses. Donc, est-ce qu'on pourrait appliquer un processus de certification de ce type concernant ces contrats, et cela en matière d'abus de DNS?

SUSAN CHALMERS : Je ne suis pas très sûre des exigences ou des procédures de l'ISO en la matière, mais on pourrait peut-être en parler après.

NICHOLAS CABALLERO : Merci, Susan. Merci, l'Indonésie. Est-ce qu'il y a d'autres commentaires ou des questions? Je vois qu'il n'y en a pas. Nous allons passer au point suivant de l'ordre du jour. Susan, vous avez la parole.

SUSAN CHALMERS : Maintenant, nous allons passer aux présentations des invités. Nous allons commencer par la présentation de l'Institut DNS Abuse.

GRAEME BUNTON : Merci beaucoup à tous, Susan. Désolée pour les gens qui étaient ici pendant le renforcement des capacités du week-end. Je m'appelle Graeme, je suis le responsable du DNS Abuse Institute. Nous nous exploitons le point Org et nous essayons dans cet institut d'essayer de résoudre des problèmes liés à l'abus des DNS dans cette industrie. Et cette activité est indépendante des activités d'exploitation du point Org.

J'ai ajouté quelques diapos par rapport à celles que je vous ai montré le week-end dernier. Alors, très brièvement, je vais vous raconter en

quoi consiste notre projet Compass et comment nous mesurons l'impact des amendements et comment nous mesurons les cas d'abus. Et je vais essayer de tout faire en huit minutes.

Nous avons créé ce projet qui s'appelle Compass. Nous sentions que la communauté de l'ICANN avait besoin de pouvoir élaborer des politiques basées sur des données et ensuite les bureaux d'enregistrement, les opérateurs de registre avaient besoin de données également. Nous voulions donc construire une approche rigoureuse et transparente pour obtenir ce type de données. C'est pourquoi nous avons lancé ce projet.

Nous fournissons des rapports mensuels en matière d’abus de DNS. Je vais vous partager le lien si vous voulez les consulter. Nous avons donc ces rapports mensuels qui incluent des données agrégées de l'industrie ainsi que le palmarès des opérateurs de registre ou bureau d'enregistrement qui ont des taux d'abus élevés et des taux d'abus très faibles.

Diapo suivante, s'il vous plaît. Ici, vous voyez, c'est une diapo très compliquée. Je sais que vous n'allez pas la digérer de suite, mais si c'est un sujet qui vous intéresse, je vous invite à une séance de la ccNSO de cet après-midi. Je serai là, Samaneh sera là et va aborder en détail cette question.

Donc l'idée, c'est de savoir comment on mesure la de DNS. Pour ce faire, il faut donc collecter un certain nombre d'informations par rapport aux abus. Cela est fait par les listes de blocage de réputation. Il s'agit de sources d'information sur l'abus des noms de domaine. Il y a certains

problèmes avec ces sources. Cela relèverait d'une discussion plus approfondie. Il faut donc nettoyer un petit peu l'information qui vient de ces sources. Ce que nous faisons, c’est que nous identifions de manière très précise ces sites. Nous utilisons un algorithme pour identifier s'il s'agit de domaines qui ont été enregistrés à des fins malveillantes ou s'il s'agit de domaines qui ont été piratés ou qui sont compromis.

Ensuite, donc, nous faisons un suivi de ces sites web à certains intervalles de temps, jusqu'à 30 jours, donc toutes les 5 minutes, ou toutes les 10 minutes, toutes les heures, toutes les 2 h, toutes les 6 h, toutes les 12 h, et cela pendant 30 jours. Cela nous permet de mesurer non seulement les pourcentages ou les taux d'atténuation, mais aussi les taux d’abus. S'il y a des TLD ou des bureaux d'enregistrement ou des opérateurs d'enregistrement dans la salle, n'hésitez pas à nous contacter si vous avez davantage d'informations. Nous fournissons donc ces informations à la communauté. Tout cela est gratuit pour les ccTLD ou les TLD ou les bureaux d'enregistrement, ils peuvent accéder à ces bureaux, à ces informations.

Diapo suivante, s'il vous plaît! Voilà un rapport sur les taux d'abus généraux. Ce ne serait pas approprié de tirer des conclusions par rapport à des tendances, car il y a eu des changements entre décembre 2022 et janvier 2023. Et cela, parce qu'il y a un fournisseur de services gratuits de TLD qui n'est plus en ligne. Donc si on sort cela de données historiques, je pense qu'on ne devrait pas voir de changements importants au niveau des tendances.

Si on pense aux amendements et à l'impact que ces amendements pourraient avoir, j'ai l'impression que sur une période longue de temps, on pourrait commencer à voir une diminution des taux d'abus parce que les bureaux d'enregistrement commenceront à faire plus par rapport à ce sujet. Cette communauté devrait penser à la conséquence de ces amendements. Où iront ces cas d'utilisation malveillante? Parce que les acteurs malveillants resteront des acteurs malveillants.

Donc ici, vous voyez donc d'autres informations de nos rapports. C'est la mesure des taux d'atténuation. Comme je vous l'ai dit, nous vérifions ces domaines au fil du temps pour voir ce qui se passe. L'atténuation peut être un domaine suspendu par un bureau d'enregistrement, un domaine suspendu par un opérateur de registre. Il peut y avoir un changement de site web ou il pourrait y avoir l'hébergeur qui serait engagé ou bien l'acteur malveillant arrête ses activités. Donc on ne parle pas de la personne qui met en place les activités d'atténuation, mais le fait que l'activité malveillante s'arrête.

Donc la couleur orange correspond au cas où on n'a pas pu détecter d'activité d'atténuation. Nous voyons qu'il y a à peu près 40 % des abus qui sont atténués dans l'industrie. Il faudra voir ce qui va se passer après les amendements. Je pense qu'on verra des améliorations au niveau de ce taux d'atténuation.

Diapo suivante, s'il vous plaît! Ici, vous voyez donc une capture d'écran de notre tableau de suivi, et vous voyez donc le temps en moyenne que prend une action d'atténuation. En général, on parle de 24 h, ce qui est un délai assez intéressant. Les parties qui seront utiles pour comprendre l'impact des amendements sont les taux d'abus en

général, les taux d'atténuation en général et la moyenne de temps d'atténuation. Donc ces informations pourront nous aider à mieux pouvoir mesurer l'impact des amendements.

Je suis assez optimiste, je dois l'avouer, mais je pense que les taux d'atténuation vont s'améliorer parce que l'industrie sera encouragée à le faire et je pense que le délai d'atténuation va se réduire également. Donc voilà tout ce que je voulais vous présenter aujourd'hui. Si vous êtes intéressés à davantage d'informations, n'hésitez pas à participer à la séance qu'on aura cet après-midi. Merci beaucoup.

NICHOLAS CABALLERO : Merci, Graeme. Est-ce qu'il y a des questions pour notre invité dans la salle ou en ligne?

GRAEME BUNTON : Je devrais ajouter une information. Nous faisons tout cela gratuitement. Donc si vous êtes un bureau d'enregistrement ou un opérateur de registre, ou si vous voulez comprendre mieux l'abus, les cas d'abus, n'hésitez pas à nous contacter.

NICHOLAS CABALLERO : Merci beaucoup, Graeme. C'est un point très important. Je vois qu'il n'y a pas de questions en ligne ou dans la salle. Alors Suzanne, vous avez la parole.

SUSAN CHALMERS : Merci beaucoup, Président. Je pense que l'idée d'utiliser ces données et ces métriques et voir comment les amendements pourront influencer ces données, c'est très intéressant et ce serait intéressant d'avoir ces discussions à l'avenir. Maintenant, je vais passer à l'organisation ICANN. Donc je vais passer la parole au département OCTO de l'ICANN.

SAMANEH TAJALIZADEKHOOB : Merci beaucoup. Je m'appelle Samaneh. Je suis directrice de recherche sur la stabilité, la résilience et la sécurité dans le bureau du directeur de la technologie de l'ICANN. Et je dirige le projet DAAR, le projet de signalement des cas d'utilisation malveillantes des noms de domaine. Cette présentation a surtout pour objectif de vous informer de nos activités.

Diapo suivante, s'il vous plaît! Donc l'outil DAAR existe depuis 2017. Il collecte les informations issues des listes de blocage et de réputation au niveau des TLD. Ces données sont agrégées au niveau des TLD. Après, on établit une cartographie avec les domaines comptabilisés par fichier de zone et on comptabilise par jour et par mois ces informations.

Cet outil permet d'établir des rapports mensuels qui sont publiés sur la page web du projet DAAR. Les registres peuvent accéder à leurs propres chiffres parce que nous avons une API qui enregistre l'utilisation de ces données. Cet outil est disponible depuis longtemps et cela nous permet de pouvoir identifier des tendances à long terme.

Vous avez là un aperçu simplifié du fonctionnement. Donc il y a les domaines de RBL qui sont énumérés, qui sont combinés et ensuite, on

traite les cas et on produit des analyses. Il y a deux types d'analyse : il y a donc le compte brut et il y a le nombre normalisé – le pourcentage normalisé. Alors j'essaye de vous expliquer comment fonctionne cet outil en termes plus simples, parce que la dernière fois que j'ai présenté l'outil au GAC, étant donné que je n'avais pas beaucoup de temps, je ne vais pas vous donner tous les détails sur cet outil, mais n'hésitez pas à me poser des questions après la présentation si je n'ai pas donné assez de détails.

Donc voilà ce qui est créé par l'outil et qui est inclus au rapport mensuel. Vous avez là la distribution par cas d'abus, par type de cas d'abus dans les gTLD historiques. Et le message de ce visuel, c'est que suivant le type de TLD, la concentration peut être différente. Donc par exemple, les domaines malveillants, il y en a un peu plus dans les TLD historiques. Pour les nouveaux TLD, c'est plutôt le pourriel.

Ensuite, vous avez là un autre exemple de dessins qui sont produits par le rapport mensuel du DAAR. Donc vous avez sur la ligne des Y le pourcentage d'abus et sur la ligne du X, vous avez la taille du TLD. Chaque cercle est un TLD. Donc, vous voyez que plus le point est élevé dans le dessin et plus le cercle est large, plus il y a d'abus dans le TLD.

Ceci n'est pas inclus dans le rapport mensuel du DAAR. Vous le voyez donc, cette ligne du temps est très longue. Je l'avais générée pour cette raison parce que je pensais que c'était intéressant, étant donné qu'elle couvre pratiquement 5 ans. Donc Voilà pourquoi le titre du X est un peu mélangé. Mais donc voici la perspective de l'ICANN sur les 5 ans en termes de collecte de données. Pour ce qui est de l'hameçonnage, des

programmes malveillants et du spam et du commandement et contrôle. Diapositive suivante.

Je sais que le projet DAAR a été perçu dans différents groupes de la communauté de l'ICANN de manière différente. Mais je crois qu'il y a certaines choses qu'un projet peut faire et certaines choses qu'un projet ne peut pas faire. En l'état actuel, le projet ne peut signaler que les activités de menace au niveau des TLD. Il peut nous donner des rapports sur les tendances, les données historiques. Il y a quatre types de menaces collectées par le système et ces données, comme elles sont cumulées et anonymisées, ne peuvent pas donner lieu à des actions immédiates, mais elles peuvent au moins indiquer où sont les concentrations des menaces.

Ce que le projet ne peut pas faire en l'état, c'est qu'il ne peut pas fournir des données au niveau des bureaux d'enregistrement, seulement au niveau des registres, et il ne peut pas donner d'informations sur les stratégies d'atténuation. Le système ne comporte pas de mécanisme pour distinguer entre les domaines compromis et les domaines enregistrés à des fins malveillantes. Il ne publie pas les noms de TLD ou de registre sur la base des abus.

Ensuite, alors qu'est-ce qu'on fait maintenant? Eh bien, cela fait pratiquement un an que le groupe sur la sécurité, la stabilité et la résilience de l’OCTO, nous avons travaillé sur ce projet et nous voulons passer au niveau supérieur. Nous avons reçu des révisions de différentes parties de la communauté. Nous avons consulté ces différents groupes. J'ai présenté à de multiples reprises ce projet à vous

et à d'autres, et donc nous sommes en train de réfléchir à l'étape suivante de ce projet.

Nous sommes en train de définir les exigences du projet. Le projet est mis en place à l'interne et il est perçu comme une plateforme de mesures, alors qu'en fait il est plus large. Donc nous allons ajouter des fonctionnalités, des modules avec le temps. Il y a beaucoup de choses que nous souhaitons faire avec ce projet. Donc nous commençons petit pour nous élargir à l'avenir. Premier module prévu, mesuré pour les opérateurs de registre et les bureaux d'enregistrement. Donc nous ajoutons ceci au système DAAR. Il y aura aussi un tableau de bord dynamique pour partager des graphiques. Il y aura une fonctionnalité de recherche pour les utilisateurs avec différents niveaux d'utilisateurs et il y aura également la possibilité pour les ccTLD de participer. Il y aura aussi une API qui donnera accès à des données venant des chercheurs et des universitaires s'ils souhaitent y contribuer.

Une fois que le premier module aura été lancé ou publié, il y aura d'autres choses de haut niveau que nous souhaitons ajouter au projet. Donc ce sont des idées, des concepts globaux. Un petit peu après le lancement du premier module, donc ce sera à peu près dans un an. Voilà donc les initiatives futures que nous considérons. Donc nous souhaitons que la plateforme fournisse des données sur les listes de blocage et de réputation qui pourront être partagées. Nous souhaitons également distinguer entre les types de domaines, soit compromis, soit enregistré à des fins malveillantes. Les domaines parqués, les prévisions de menaces…

Les chercheurs à l'équipe SSR travaillent sur la science derrière chacun de ces modèles. Chaque année, nous devrions ajouter un modèle au système. Donc davantage d'informations seront partagées dans la séance ccTLD de cet après-midi qui a déjà été mentionné par Graeme. Et si vous avez des questions, n'hésitez pas, je peux y répondre.

NICHOLAS CABALLERO : Merci beaucoup, Samaneh. Est ce qu'il y a des questions? J'ai l'Inde. Allez-y.

T. SANTHOSH : Merci, monsieur le Président. Excellente présentation donc de la part du DNS Abuse Institute et de la part de la dernière intervenante. J'aimerais savoir si l'ICANN atténue l'utilisation malveillante du DNS par le DNS sur HTTPS ou le DNS sur TLS parce qu'il est très difficile de détecter le trafic. Est-ce que vous pourrez détecter les domaines malveillants grâce à DOH ou DOT?

SAMANEH TAJALIZADEHKOOB : Merci pour la question. La question que vous posez comporte deux niveaux. Il y a la partie détection. Ce que vous dites, ce à quoi vous faites référence, c'est un mécanisme qui utilise le DOT ou le DOH pour faire la détection. Ceci implique une entité qui fait la détection dans le cadre du projet DAAR. Nous avons d'autres projets qui nous permettent de détecter. Mais pour le projet DAAR, nous ne faisons pas la détection nous-même. Nous utilisons les domaines qui nous sont signalés par d'autres parties tierces. Donc, nous ne sommes pas impliqués dans le

processus de détection. Nous prenons les domaines qui sont listés sur les listes, qui sont répertoriés, sur les listes de réputation et de blocage, et nous faisons davantage d'investigations pour trouver les preuves d'abus.

NICHOLAS CABALLERO : Merci à l'Inde. J'ai la Chine.

WANG LANG : Merci Nico. Wang Yang, représentant du GAC au micro. Nous savons qu'il y a un comité sur l'utilisation malveillante du DNS à la ccNSO. Il s'agit d'un comité permanent. Il y a également un petit groupe à la GNSO qui s'occupe des questions d'utilisations malveillantes du DNS. Quelle est la différence entre ces deux groupes, la différence entre leurs responsabilités, entre et aussi les différences peut-être de résultats?

NICK WENBAN-SMITH : Je serais ravi d'en parler, mais je pense que je vais en parler pendant la présentation que je vais faire. Donc si vous le voulez bien, écoutez ma présentation et si vous avez encore des questions, vous pourrez les poser après.

NICHOLAS CABALLERO : Merci à la Chine. Y a-t-il des questions dans la salle ou en ligne? Personne. Pardon? L'Inde? Allez-y.

SUSHIL PAL : Est-ce que vous prévoyez d'entrer en lien avec les pays qui subissent des attaques multiples? Peut-être un renforcement des capacités ou entrer en lien avec ces pays pour les aider à prendre toutes les précautions nécessaires?

SAMANEH TAJALIZADEHKHOOB : Oui, alors du point de vue de l'OCTO, il y a une équipe relation technique. Peut-être d'ailleurs que vous les avez déjà contactés et que vous avez travaillé avec eux. Nous, à SSR, on travaille avec le point IN, point indien dans le cadre du projet DAAR. Donc je sais que nous travaillons déjà avec vous, mais on peut toujours après la réunion, entrer en contact si vous avez besoin de formation et je vous mettrai en contact avec l'équipe.

GRAEME BUNTON : On était récemment au Vietnam. On a organisé une séance de renforcement de capacités avec les bureaux et opérateurs de registre et nous sommes là pour éduquer tous ceux qui en ont besoin, pour former les gens. Donc n'hésitez pas à nous contacter. Nous travaillons également pour rassembler davantage de partenaires dans le cadre de NetBeacon, qui est un service que nous fournissons également pour les signalements d'abus.

NICHOLAS CABALLERO : Merci beaucoup, Graeme et Samaneh Tajalizadehkhoob. Je ne sais pas si je prononce bien votre nom, il est assez long. D'autres questions? Sinon, je vais donner la parole à Chris. Chris?

CHRIS LEWIS-EVANS : Merci Nico. Donc Chris Lewis-Evans. Je suis très heureux de m'adresser à vous. J'avais un manque parce que je parlais toujours en tant que PSWG et maintenant je suis à la relation avec les gouvernements et donc nous nous occupons de tout ce qui est utilisation malveillante du DNS pour les bureaux d'enregistrement, opérateurs de registre, services d'hébergement. Et donc nous nous occupons des signalements d'utilisation malveillantes DNS, tout ce qui est rapports qui nous aident à avancer en termes d'atténuation.

Alors premièrement, la première chose qui est clé, c'est de recevoir des rapports. On en a déjà parlé. Le problème, c'est le manque de signalement, l'absence de signalement dans nos différents pays. Je crois que c'est quelque chose de standard. Donc les outils tels que le Net Beacon, que Graeme a mentionné à l'instant, c'est très important. Nous alimentons le NetBeacon en tout cas. Merci Graeme. Et puis les listes d'abus aussi. Graham les a mentionnées. Les listes d'abus ont parfois besoin d'être nettoyés. Elles ne sont pas cohérentes, elles ne sont pas très bien alimentées. Pourtant, ceci ajoute aux preuves d'abus si on arrive à avoir différentes sources.

Nos clients ont des formulaires pour signaler les utilisations abusives et donc bureau d'enregistrement, opérateur de registre et service d'hébergement. Donc nous recevons ceci de leur part. Ils nous envoient ces formulaires directement. Et il y a aussi tout ce qui est cybersécurité. Beaucoup d'informations sont à leur disposition. Ils détectent énormément d'abus, donc on reçoit les informations des services gouvernementaux.

Je sais que le Royaume-Uni a un projet de signalement des emails suspects qui sont utilisés, par exemple pour les vols ou pour l’hameçonnage. Et donc obtenir ces informations des sortes et autres est quelque chose de très utile pour nous, pour atténuer.

Donc je continue sur ces questions de signalement parce que c'est très important. Au CleanDNS, nous comprenons bien qu'il est important d'atténuer autant que possible et aussi rapidement que possible. Nous recevons des signalements d'abus d'un peu partout, de tous les opérateurs de registre, bureaux d'enregistrement ou hébergeurs. Lorsque nous les recevons, nous les traitons et nous traitons les preuves. Si c'est un client, nous nous en occupons. Sinon, nous renvoyons ceci à la partie appropriée en utilisant le NetBeacon du DNS Abuse Institute et eux informent la partie concernée.

Une des choses qu'on a pu observer dans la recherche et qui est très importante dans le cadre du signalement, c'est le feedback. Ceux qui signalent n'aiment pas signaler et ensuite voir les choses disparaître dans un trou noir sans savoir ce qui s'est passé, surtout lorsqu'on a été victime. Il est vraiment important de voir qu'il y a quelque chose qui est fait quand on a signalé. Donc nous les informons de ce qui a été fait par rapport au domaine et ceci nous permet d'avoir davantage en fait de conséquences positives, parce que les gens continuent de signaler.

Et dernier point, Graeme en a parlé, et je crois que c'est une clé pour l'atténuation des abus. Il s'agit du temps jusqu'au moment où on supprime. C'est vraiment la clé. Il faut que ce soit rapide de manière à minimiser le nombre de victimes. Donc je crois que le temps ou le délai est important. Il est difficile de mesurer toutes les conséquences

négatives d'un programme malveillant si on n'a pas agi rapidement. Nous avons des preuves qui sont différentes suivant les types d'abus. Un email d’hameçonnage, ce n'est pas la même chose qu'un site qui a déployé un programme malveillant.

Donc on ne peut pas collecter les preuves de la même manière. Il faut pouvoir qualifier chacun des préjudices. Très souvent, on peut donner un aperçu visuel, mais pas tout le temps. Le téléchargement d'un programme malveillant, c'est difficile de prendre une capture d'écran de ce type de choses. Donc il y a des procédures et des pratiques à mettre en place.

Donc il faut toujours avoir un enregistrement de preuves exploitables qui ensuite peuvent être envoyé aux parties appropriées qui peuvent agir. Donc, j'ai énuméré ici un nombre de choses que nous pouvons faire. Donc déjà le rapport, le signalement est important parce que cela montre l'impact, le préjudice initial, ensuite les captures d'écran. Beaucoup d'informations URL condensées également. Alors attention, bien sûr, ne téléchargez pas le programme malveillant pour l'envoyer dans le cadre de votre rapport. On ne veut pas que vous vous exposiez à ce danger. Et puis toutes les métadonnées également sont très importantes.

À partir de cette liste, la question que l'on reçoit, c'est que les listes contiennent beaucoup d'informations à caractère personnel ou d'identification. Nous ne collectons pas les informations à caractère personnel, nous ne les mettons pas dans les rapports pour prouver cette utilisation malveillante. Autant que possible, nous essayons d'automatiser, de travailler rapidement, de collecter toutes les

informations, de les combiner pour en fait avoir quelque chose d'exploitable pour que l'hébergeur, le bureau ou l'opérateur puisse agir de manière appropriée.

Par rapport à la mesure entreprise, nous n'intervenons pas parce que souvent, la personne la plus appropriée, qui doit donc engager la mesure, c'est le titulaire du nom de domaine. Donc on est en contact avec le bureau d'enregistrement qui contacte le titulaire de nom de domaine. Ou alors si c'est un hébergeur, on va utiliser le WHOIS pour obtenir les données et pour ensuite aider la personne à s'occuper de ce problème de domaine compromis.

Voilà, donc je ne sais pas s'il y a des questions, sinon je le ferai à la fin.

NICHOLAS CABALLERO : Merci beaucoup, Chris. Je vais maintenant vous passer la parole pour vos questions, vos commentaires en ligne ou dans la salle.

LAUREEN KAPIN : Très rapidement. Vous l'avez déjà entendu, mais je voulais souligner cela. Les derniers intervenants nous ont aidés à faire cette séance et ils ont pu intervenir alors qu'on les a invités il n'y a pas longtemps. Donc je tenais à les remercier.

NICHOLAS CABALLERO : Je voulais justement applaudir ces présentations qui ont été faites. Mais j'ai déjà deux personnes qui souhaitent prendre la parole. J'ai l'Inde et l'Iran. Allez-y, l'Inde, si vous souhaitez prendre la parole.

T. SANTOSH : Santosh pour les enregistrements. Ma question concerne le processus SubPro et la piste de travail sur les nouveaux gTLD ainsi que la piste de travail sur le WHOIS. Nous recevons des informations actualisées de la part du secrétariat, mais pour tout ce qui est des abus de DNS, nous devons nous rendre sur le site de l'organisation ICANN pour obtenir des informations. Je souhaite demander au secrétariat du GAC de bien vouloir partager des informations par mail à tous les représentants du GAC, ce type d'information sur l'abus de DNS. Merci beaucoup. Ce serait très utile.

NICHOLAS CABALLERO : Merci l'Inde. L'Iran, s'il vous plaît.

KAVOUSS ARASTEH : Je rejoins ce que vient de dire Laureen pour ce qui est des remerciements. C'était vraiment des présentations très informatives. J'aimerais savoir quelles sont donc les actions que l'on peut mettre en place une fois que ces cas d'abus du DNS ont été identifiés. Qu'est-ce qui se passe au niveau des feedbacks? Comment on revient vers les personnes qui ont signalé tout cela? Ce serait très intéressant de connaître toutes ces informations parce qu'on nous a fourni énormément d'informations hier, aujourd'hui, par rapport à l'utilisation malveillante du DNS, et donc nous aimerions savoir ce qui se passe après. Merci beaucoup.

NICHOLAS CABALLERO : Chris, est ce que vous souhaitez répondre?

CHRIS LEWIS-EVANS : Ce que nous pouvons faire, c'est soutenir les bureaux d'enregistrement et les opérateurs de registre pour accepter les changements contractuels. Je crois que le Canada l'a très bien dit au début de la séance. C'est un pas énorme qui est fait parce que cela nous permet de faire des progrès au niveau de la lutte contre l'utilisation malveillante du DNS. C'est un pas en avant très important et nous saluons cette initiative.

SUSAN CHALMERS : Kavouss, je suggère que l'on retourne vers la liste de diffusion du GAC. Il y a beaucoup d'informations, notamment en amont de la réunion de San Juan. Donc je vous encourage à participer à cette liste de diffusion pour promouvoir des discussions.

NICHOLAS CABALLERO : L’Iran, s'il vous plaît.

KAVOUSS ARASTEH : Merci beaucoup pour cette réponse. Oui, notre collègue du Canada a parlé des intervenants qui se trouvent en dehors du système de l'ICANN – les bureaux d'enregistrement, les opérateurs de registre. Comment pouvons-nous faire pour obtenir une influence, une participation ou jouer un rôle actif dans cette question qui est en dehors de l'ICANN?

Quels sont donc les besoins pour pouvoir participer plus activement dans ce domaine?

SAMANEH TAJALIZADEHKHOOB : Du point de vue de la recherche d'abus en matière de DNS, vous pouvez participer au projet DAAR. Tous les ccTLD peuvent participer à ce projet. Donc si vous vous portez volontaire pour participer, vous devez fournir le fichier de zone et à ce moment-là, vous allez recevoir des rapports mensuels. Le groupe TE fournit également des formations ou assure des formations de renforcement de capacité par rapport aux ressources dont nous disposons et qui peuvent aider les ccTLD.

NICHOLAS CABALLERO : Merci Samaneh. D'autres questions ou d'autres commentaires? C'est vraiment une question fascinante, mais on ne dispose pas de beaucoup de temps. Donc je vais donner la parole à Nick pour qu'il aborde le point suivant de l'ordre du jour.

NICK WENBAM-SMITH : Est-ce qu'on peut afficher mes diapositives, s'il vous plaît? Très bien, merci beaucoup. Donc un aperçu de ce que je ce dont je vais parler. Je vais vous parler de la ccNSO et du DASC. C'est le comité permanent sur l'utilisation malveillante du DNS. Nous fournissons des outils pour les ccTLD.

Il s'agit d'un projet qui se penche surtout sur les pratiques de la communauté ccNSO. Nous avons pu mener une enquête. Nous avons pu tirer des conclusions très intéressantes et nous sommes très

reconnaissants aux gens qui ont promu une séance de cet après-midi. C'est un domaine assez complexe et donc plusieurs présentations seront faites à partir de différents points de vue. Il y aura une séance cet après-midi où des informations plus détaillées seront données. Diapo suivante.

Pour un moment, je vous demande de ne pas penser aux gTLD, aux SubPro, aux amendements aux contrats. Tout cela ne fait pas partie de ma présentation. Ici, on va parler des codes de pays. Mon rôle? Je travaille avec le point UK, le ccTLD. Je travaille dans le domaine de la cybercriminalité depuis plus de 15 ans, mais c'est pourquoi je suis le président de ce comité permanent qui s'occupe de l'utilisation malveillante du DNS.

Donc vous voyez, il y a une énorme diversité, il y a des IDN. Il y a plus de 300 ccTLD au total si on inclut les variantes IDN. Vous voyez, c'est un monde très diversifié. Et nous n'avons pas de contrat avec l'ICANN. Nous sommes souverains. Nous n'aurons jamais de contrat avec l'ICANN. Nous reflétons donc la diversité du monde. Diapo suivante, s'il vous plaît! Très bien.

Donc nous ne sommes pas là pour élaborer des politiques. Ces politiques sont élaborées par chaque ccTLD. Nous, notre but est de partager des informations et essayer de mener des activités de sensibilisation. Nous avons une communauté très forte qui partage beaucoup d'informations et fondamentalement, nous voulons faire de notre mieux pour atténuer les cas d'utilisation malveillante dans des TLD. C'est pour cela que nous essayons de faire en sorte de diminuer les niveaux d'abus en général.

Quelles sont les ressources que nous mettons à disposition? Tout d'abord, un référentiel. Avec David McAuley de VeriSign, nous fournissons un ensemble de ressources qui sont utiles pour la communauté des ccTLD concernant l'utilisation malveillante du DNS. Nous encourageons les membres à cliquer sur les liens qui figurent sur l'écran si vous voulez obtenir davantage d'informations. Diapo suivante, s'il vous plaît!

Nous avons également une liste de diffusion dédiée. Ce sera une nouvelle ressource pour que la communauté ccTLD puisse être mieux connectée et puisse partager des informations de manière plus rapide. Ce n'est pas confidentiel, mais cela est partagé par les membres qui ont des ccTLD.

Voilà la diapo sur laquelle je voulais m'attarder un petit peu plus. En 2022, nous avons mené une enquête auprès des opérateurs de ccTLD par rapport à la question de l'abus de DNS. Il faut se rappeler que la ccNSO est assez large. Nous avons reçu 57 réponses uniques. Ce n'est pas une enquête obligatoire que nous avons menée et donc il faut se souvenir que c'est un petit groupe qui a répondu à cette enquête.

Pour encourager la participation, nous avons donc respecté un certain nombre de critères de confidentialité dans cette enquête. Donc nous avons présenté les détails de l'enquête à trois reprises dans différentes sessions. Cette enquête a été très intéressante et très utile pour guider les activités que nous allons mettre en place à l'avenir et pour mieux comprendre quelles sont les problématiques auxquelles est confrontée la communauté des ccTLD.

Comme je vous le disais, c'était très intéressant. Les ccTLD constituent un groupe très diversifié. Bien sûr, les pays sont différents. Donc il y a un large éventail de ccTLD avec différents modèles de gouvernance, différents niveaux d'abus, avec des variations régionales bien entendu, mais déjà au niveau national, il y a énormément de variations. Diapo suivante, s'il vous plaît.

Lors de l'ICANN76 à Cancun, les résultats de l'enquête se sont concentrés sur les mesures que les différents ccTLD mettent en place lorsqu'ils sont confrontés à des cas d'abus. Parce que, à ce qu'il paraît, ce n'est pas les mêmes types de pratiques d'atténuation partout. Et c'est intéressant à constater parce que – prenez mon exemple – nous ne définissons pas l'abus de DNS, nous avons criminalité et abus. Voilà les questions sur lesquelles nous agissons en fonction de ce qui s'est passé et donc en fonction de ce qui s'est passé, les actions d’atténuation sont différentes.

Donc voilà, c'est un exemple intéressant. Beaucoup d'entre nous nous penchons sur l'abus à partir d'une évaluation de risque et donc à ce moment-là, nous pouvons soit suspendre, soit éliminer le domaine. Ensuite, lors de l'ICANN77, nous nous sommes focalisés sur les différents modèles de registre. Certains ccTLD ne s'engagent pas à enregistrer sans avoir préalablement collecté un certain nombre d'informations.

Donc nous avons essayé de voir s'il y a une corrélation entre ces informations collectées avant l'enregistrement ou la validation de ces données. Nous ne le faisons pas, mais nous voulions voir s'il y a une corrélation entre une validation de données en amont de

l'enregistrement et des taux d'utilisation malveillante. Et ça a été un exercice vraiment fascinant.

Alors, je veux mettre l'accent sur un élément et vous vous souviendrez de ma présentation que j'ai dit que les ccTLD sont presque les TLD, les noms de domaine les plus sûrs. Nous avons mené cette analyse à partir des informations que nous avons collectées. Nous avons vérifié avec les données collectées par l'Institut DNS Abuse avec les données fournies par les différents ccTLD.

Et l'une des raisons pour lesquelles nous avons cette séance cet après-midi, c'est justement pour voir comment nous mesurons les abus. Quels sont les outils et les procédures qui sont disponibles? Pourquoi nous faisons cela? Parce que 38 % des répondants à l'enquête nous ont dit qu'ils n'étaient pas sûrs ou ils ne savaient pas vraiment quel est quel était le taux d'abus de leur ccTLD. C'est pour cela que nous voulons insister sur cela, car tous les ccTLD devraient avoir ces informations et savoir comment mesurer l'abus dans leur propre système et être au courant de quelles sont les actions que vous pouvez mettre en place pour réduire ces cas d'abus.

L'une des raisons pour lesquelles les gens n'étaient pas sûrs par rapport au taux d'abus dans leur ccTLD, c'est parce que dans certains petits ccTLD, il y a beaucoup de vérifications qui se font au moment de l'enregistrement. Et donc le taux d'abus du DNS est tellement petit qu'il est très difficile à constater. Parfois, c'est près de zéro. Ce sont des niveaux vraiment très faibles. Et donc certains des répondants avaient raison pour nous dire nous ne sommes pas sûrs parce que nous ne

pouvons pas les constater, ces taux de l'utilisation malveillante du DNS. Et c'était intéressant comme conclusion. Diapo suivante.

Personnellement, j'ai toujours suspecté comment ça se passait les modèles d'enregistrement gratuits. Une des hypothèses, c'est que les noms de domaine pas chers du tout ont une corrélation avec des niveaux d'abus élevés. Nous essayons de trouver une corrélation. Donc nous sommes à Hambourg, nous sommes en Allemagne.

C'est l'un des ccTLD, l'un des ccTLD les plus importants ou les plus grands. C'est point DE qui fonctionne très bien. Nous sommes en Allemagne, ils ont beaucoup de domaines et c'est très bon marché. Ce n’est pas cher du tout de pouvoir enregistrer un domaine sous point DE. Et pourtant les taux d'abus sont très faibles pour ce domaine. Donc ce n'était pas facile de trouver une corrélation entre des noms de domaine pas chers et des activités malveillantes. C'était intéressant donc de tirer cette conclusion.

Et maintenant je vais conclure. Diapo suivante, s'il vous plaît! Nous avons organisé un webinaire où nous avons abordé un certain nombre de questions : la variation entre les ccTLD. Ensuite, la définition d'abus établie par l'ICANN. Parce que pour les ccTLD, cette définition n'est pas la même que celle qui est établie par l'ICANN. Donc il y a une diversité de définitions. Il y a une définition du côté technique et une définition du côté politique. Donc, comme je vous le disais, les ccTLD affichent des niveaux très faibles d'abus du DNS. Il y a différentes façons de répondre à ces abus. Chaque ccTLD le fait de manière différente. Les vérifications au moment de l'enregistrement. C'est un domaine très intéressant à observer et nous menons un certain nombre de validations non

seulement pour éviter les abus de DNS, mais aussi parce que nous souhaitons que nos données soient exactes. C'est l'objectif principal. Diapo suivante, s'il vous plaît!

Et finalement, moi aussi, j'ai ce problème des diapos qui se suivent très vite. Donc cet après-midi, on va consacrer 2 h dans une séance qui va porter sur les outils et la mesure des abus du DNS. On aura des présentations très intéressantes de l'équipe OCTO du projet DAAR. Il y a une collaboration également entre deux ccTLD, belge et des Pays-Bas, qui utilisent des techniques d'intelligence artificielle pour mieux prédire les cas d'abus du DNS.

Et pour répondre à la question de la Chine tout à l'heure, cette séance sera suivie d'une discussion entre moi-même et Bruce Tonkin, qui est le vice-président de ce comité DASC, le groupe de représentants des opérateurs de registre. On aura une discussion sur la mesure d'abus dans les ccTLD et les gTLD. Il y a des opérateurs de registre qui s'occupent également de TLD, des ccTLD et des gTLD. Donc l'idée c'est de coordonner le travail entre tous les TLD pour pouvoir obtenir des résultats positifs à tous les niveaux. Diapo suivante, s'il vous plaît. Vous pouvez voir quels sont nos plans pour l'avenir, donc avoir des politiques d'enregistrement et de validation pour tous les ccTLD.

Il y a une coopération qui doit se mettre en place entre les bureaux d'enregistrement et les opérateurs de registre. C'est aussi un domaine intéressant sur lequel nous pouvons nous pencher. Et voilà donc nos plans pour l'avenir et c'est la fin de ma présentation. Maintenant, je repasse la parole à Nico.

NICHOLAS CABALLERO : Merci beaucoup, Nick Est-ce que le GAC a des questions, des commentaires sur ce sujet pour Nick? Le Japon? Allez-y.

NISHIGATA NOBUHISA : Merci beaucoup pour cette excellente présentation. J'ai deux questions à vous poser par rapport à votre opinion. Premièrement, j'ai vu qu'il y avait de bonnes pratiques pour prévenir ou décourager l'utilisation malveillante du DNS via le ccTLD. Est-ce qu'il y aurait moyen d'exploiter ces bonnes pratiques de ccTLD pour peut-être inspirer des… ou donner des idées aux bureaux d'enregistrement et opérateurs de registre. Donc utiliser ces bonnes pratiques pour prévenir ou décourager toute conduite malveillante sur Internet.

Deuxième question. Il y a une certaine diversité dans les ccTLD, dans les pays. Donc vous avez présenté de bonnes pratiques dans des pays tels que l'Allemagne. Mais je crois qu'il y a aussi des pays où les ccTLD, parfois ont des domaines qui se conduisent de manière malveillante. Donc y a-t-il d'autres activités de votre point de vue qui pourraient en fait convaincre ces pays de décourager ce type de choses?

NICK WENBAN-SMITH : Merci pour cette question. Par rapport à votre première question, notre philosophie, c'est de montrer l'exemple. Mais les ccTLD ont très souvent une sorte de constitution qui décrit l'intérêt public, le bien public. Mais la réputation est très importante, me semble-t-il. Donc en encourageant les bonnes pratiques, les gens voient ces avantages qui

sont liés à une bonne réputation. C'est bon pour le pays, c'est bon pour l'économie numérique, ça permet une meilleure croissance. Donc la réputation, c'est vraiment important.

Si vous voyez qu'il y a de bons exemples, l'idée, c'est que les gens vont regarder ces exemples et les dupliquer. Donc partager les bons exemples, c'est quelque chose qui fonctionne parce que les gens vont faire les choses comme il faut en principe.

En termes de gTLD, par rapport à votre seconde question, on ne peut pas créer les politiques pour les gTLD. Mais n'oublions pas qu'il y a beaucoup de bons gTLD qui vont au-delà du minimum requis par l'ICANN et donc c'est très bien. Donc je crois qu'il faudrait que les gens adoptent les pratiques volontairement, simplement parce que c'est la bonne chose à faire, pas à cause de réglementations. Je crois que c'est la réputation. Nous ne pouvons survivre que si nos TLD sont de qualité et je pense que c'est un bon moyen d'encourager les bonnes conduites.

NICHOLAS CABALLERO : Merci beaucoup, Nick. Effectivement, la réputation c'est très important. On pourrait revenir aux Romains et à Jules César dans tout ça, mais j'ai le Taipei chinois. Allez-y!

KEN-YING TSENG : Ma question est courte : Y a-t-il des mesures préemptives en matière de l'utilisation malveillante des DNS qui sont entreprises par les ccTLD qui sont peut-être différentes des autres TLD?

NICK WENBAN-SMITH : Excellente question. Je crois qu'il y a beaucoup de points communs. Je ne pense pas qu'il soit possible de généraliser. Certains gTLD sont très proches, très spécifiques, par exemple la pharmacie ou le point Banque. Ils n'ont pas d'utilisation malveillante de DNS parce qu'ils font. Ils font beaucoup d'enregistrements.

Donc il y a des vérifications qui sont faites dans certains ccTLD. Notre philosophie, par exemple en Allemagne, est tout à fait similaire à celle des gTLD en termes de surveillance et de licences d'approbation. Mais il n'y a pas que les ccTLD qui font des choses qui soient mieux.

Mais si je réfléchis, je suis un petit peu surpris parce que les ccTLD, je ne sais pas quelle est la proportion, mais c'est peut-être un dixième des abus qui sont observés et donc en termes d'outils de mesure, j'aimerais bien comprendre comment ça se fait. Je n'arrive pas vraiment à le comprendre. Bien sûr, les Britanniques sont très honnêtes et n'ont pas de criminels. Non, il y a quelque chose qui se passe et j'aimerais bien vraiment comprendre ce qui se passe et qui fait que les ccTLD sont aussi bons. En tout cas, merci pour la question.

NICHOLAS CABALLERO : Merci pour la question et pour la réponse. Chris, allez-y

CHRIS LEWIS-EVANS : Je ne vais pas faire son boulot pour lui, mais je crois qu'il y a quand même une différence entre les ccTLD et les gTLD. Actuellement, il y a un centre qui a été créé pour le partage d'informations, le centre de partage des informations. C'est une clé, me semble-t-il, pour déjà

comprendre quels sont les types d'abus et quelles sont les pratiques que l'on peut partager entre les différents ccTLD. Et je crois que l'idée, c'est d'élargir ceci. Ce serait une bonne étape et on en a déjà parlé au GAC.

NICK WENBAN-SMITH : Oui, je crois que c'est important effectivement. Nous avons parlé de l'abus du DNS en utilisant un prisme très étroit. Mais il faut aussi parler de cybersécurité, que ce soit infrastructure, résilience ou autre type de criminalité de manière plus holistique. Et je crois que les ccTLD, nous avons des entités de partage, des informations qui nous permettent de traiter de la cyber résilience, de la cybersécurité et je pense que ça peut faire partie de la réponse.

NICHOLAS CABALLERO : Merci Chris. D'autres questions, d'autres commentaires? Personne en ligne? Si c'est le cas, je vais de nouveau céder la parole à Susan Chalmers des Etats-Unis. N'oubliez pas que c'est vous qui allez nous empêcher d'aller au déjeuner. Mais je vous embête, Susan.

SUSAN CHALMERS : Très brièvement. Graeme, Nick, Samaneh, Chris, merci beaucoup de nous avoir consacré un peu de temps pour nous informer pendant cette séance sur ces questions. Nous apprécions énormément. Que vous soyez titulaires de noms de domaine, utilisateur final ou gouvernement, nous encourageons les bureaux d'enregistrement et les opérateurs de registre à voter en faveur des amendements. Je vous remercie.

GULTEN TEPE : Merci Susan. Avant de conclure la séance. Nico, je suis vraiment désolé de vous interrompre, mais nous avons l'Iran.

NICHOLAS CABALLERO : Ah! Allez-y, l'Iran.

KAVOUSS ARASTEH : Merci. Désolé, je sais que vous devez partir au déjeuner, mais pendant cette discussion qui était très utile et très importante, il a été fait référence à plusieurs reprises à la cybersécurité et aux cyber menaces, etc. Et ceci a un impact direct sur le DNS et sur l'utilisation malveillante du DNS. Si et seulement si on doit prendre ceci en compte, je suis un peu surpris que dans d'autres domaines, en dehors de l'ICANN, il y a une certaine réticence de la part de certains gouvernements qui sont présents à cette même réunion à faire quoi que ce soit en termes de cyber menaces et de cybersécurité en ce qui concerne le DNS.

Donc, nous, en tant que membres du GAC et des gouvernements, nous devons agir. On ne peut pas en fait être ambigus, soit il y a un impact, soit il n'y a pas d'impact. Si c'est en dehors de l'ICANN, il y a par exemple à l’IUT un groupe qui s'occupe du DNS, des IDN. Et il y a eu une proposition qui a été faite, il y a eu un rejet d'un pays. Je ne vais pas nommer le pays, mais il y a eu un rejet, un refus.

Donc je crois qu'il faut avoir des positionnements communs, ne pas porter de casquette, ne pas avoir un positionnement ambigu sur le même sujet.

NICHOLAS CABALLERO : Merci beaucoup, l'Iran. Est-ce que quelqu'un souhaite répondre? Nous n'avons absolument plus de temps. Merci pour votre commentaire, l'Iran. Nous applaudissons nos intervenants qui ont été excellents aujourd'hui. Nous allons donc maintenant partir pour la pause du déjeuner.

[FIN DE LA TRANSCRIPTION]