YEŞIM SAĞLAM : Bon après-midi, bonsoir à tout le monde. Bienvenue à cet appel du groupe de travail sur les politiques consolidées. Nous sommes le 17 mai 2023 à 13 h UTC.

Nous n'allons pas faire l'appel car nous avons un temps imparti. Toutes les personnes dans la salle Zoom seront enregistrées. Nous avons reçu les excuses de Maureen Hilyard, de Steinar Grøtterød, de Mouloud Khelif, de Judith Hellerstein, de Cheryl Langdon-Orr, de Claire Craig, de Greg Shatan et de Chantelle Doerksen qui ne peuvent pas participer.

Aujourd'hui du personnel, nous avons Heidi Ullrich et moi-même, Yeşim Saglam. Je vais gérer l'appel. Comme d'habitude nous avons l'interprétation en espagnol et en français. Nous avons Claudia et Marina sur la chaîne espagnole et nous avons Dominique et Isabelle sur la chaîne d'interprétation en français.

Des rappels. Avant de commencer, nous avons un lien pour la transcription en direct. Je partage ce lien avec vous dans la boîte du chat. Autre rappel : lorsque vous prenez la parole, donnez votre nom pour la transcription mais aussi pour des interprètes.

Avec cela, je voudrais maintenant repasser la parole à Olivier. Merci beaucoup.

OLIVIER CRÉPIN-LEBLOND : Je vous remercie, Yeşim, pour cette introduction.

Bienvenue à cet appel. Aujourd'hui, nous allons faire une présentation et nous allons avoir Graeme Bunton, le directeur de l'Institut sur l'utilisation de malveillance du DNS. Vraiment, nous sommes impatients de partager avec lui cette présentation qui va prendre à peu près 40 minutes. Ensuite, nous allons parler de ce que fait le groupe de travail, des mises à jour, du processus pour le PDP des domaines internationalisés. Nous allons parler aussi du soutien aux candidatures. Après, nous allons passer un moment sur les mises à jour et nous allons parler du nouvel accord renouvelé de .net. Après cela, nous allons parler de l'ICANN77.

Y a-t-il des éléments à rajouter à l'ordre du jour ou des choses que nous devrions modifier plus tard si vous n'êtes pas encore présents sur cet appel, à savoir s'il y a quelque chose que l'on peut faire pour changer cet ordre du jour ? Je ne vois personne qui lève la main, donc je pense que nous pouvons continuer.

Il y a une question dans le chat sur un lien pour le rapport DNS AFRINIC. Mais je ne sais pas, je ne peux pas vous dire.

Nous avons un élément qui reste de l'ordre du jour de la semaine dernière. Il s'agit de la version préliminaire sur la proposition de renouvellement pour les registres. Tout le reste, sachez que tout est complété, à moins, bien, sûr qu'il y ait des commentaires ou des questions sur tout cela. Je ne vois aucune main levée. Très bien, merci.

Je vois qu'Heidi dans chat a marqué que le personnel prend note de la requête qui a été faite au niveau du point d'action. Merci Heidi.

Maintenant, nous allons passer la parole au présentateur de la journée. Il s'agit de Graeme Bunton. C'est la première fois que Graeme participe à un de nos appels. Il va nous parler de ce qu'il fait et sur quoi travaille l'Institut sur l'utilisation malveillante du DNS. Sans attendre, je vais passer la parole à Graeme.

GRAEME BUNTON : Merci. Je vais envoyer ma vidéo à Jonathan pour qu'il puisse l'enregistrer, mais nous allons la commencer dans une minute. En attendant, je vais faire une petite introduction. Est-ce que ça vous va, Jonathan ?

JONATHAN ZUCK : Oui, ça me va.

GRAEME BUNTON : Très bien.

Nous allons fonctionner de cette façon. Je vais faire des allers-retours avec la vidéo, nous allons l'envoyer à Jonathan, il va enregistrer cette vidéo et ensuite, tout le monde pourra la revoir.

Je voudrais réserver un peu de temps à la fin de ma présentation pour partager des questions et des réponses et pour passer un peu temps sur les autres activités liées à l'utilisation malveillante du DNS.

En introduction, avant de commencer, je m'appelle Graeme, je suis directeur de l'Institut sur l'utilisation malveillante du DNS et du projet qui est en cours sur les registres d'intérêt public. Nous essayons de travailler sur les noms de domaine malveillants sur l'Internet. Comment allons-nous faire cela ? Comment pouvons-nous lancer ce projet ? Comment pouvons-nous travailler ? Aujourd'hui, on va parler de cela. On a d'autres projets en cours, bien sûr, dont je parlerai.

Aujourd'hui, je suis à Barcelone. Je vis toute l'année à Toronto au Canada, mais je suis à Barcelone et j'essaie en ce moment de travailler avec différents groupes ici en Europe pendant ce séjour. Pour cette démonstration, sachez que cela va être assez court. C'est un outil qui peut être utilisé par tout le monde. Nous allons parler pendant 40 minutes et ensuite, nous aurons des

allers-retours, des questions et nous allons voir comment nous pouvons utiliser cet outil dans l'avenir.

Avec cela, je vais commencer. Je vais passer ma vidéo à Jonathan. Est-ce que vous êtes prêt, Jonathan ?

JONATHAN ZUCK : Oui, je suis prêt. Yeşim va passer ma vidéo sur l'écran. Très bien. Graeme, vous devez partager votre écran maintenant.

GRAEME BUNTON : Voilà une démonstration pour un service que nous appelons NetBeacon. NetBeacon est un outil gratuit pour tout le monde. C'est un système centralisé. Nous avons créé ce système parce que nous savons que les rapports de ces abus ou de ces utilisations malveillantes en ligne sont compliqués. Souvent, c'est difficile à faire pour les utilisateurs finaux. Nous essayons de retirer cet obstacle pour eux. Ce sont des rapports qui sont envoyés aux opérateurs de registre et aux bureaux d'enregistrement.

Souvent, il y a un manque de structure, un manque d'éléments probants. Ce qu'on essaie de faire, c'est de construire un système intermédiaire pour simplifier le processus des gens qui font rapport de ces utilisations malveillantes pour que ces

personnes puissent gérer cette utilisation malveillante par la suite.

C'est disponible en ligne. Le site netbeacon.org est assez autogérable, il est très facile à suivre. Il s'agit juste de cliquer sur ce bouton qui dit « Report Abuse » et là, vous arrivez à une page qui ressemble à cela. Comme vous voyez, vous pouvez vous mettre en ligne avec Google, mais bien sûr nous allons essayer d'intégrer d'autres manières de s'enregistrer pour simplifier les choses. Nous pensions à Apple, nous avons considéré Twitter et potentiellement peut-être même Facebook. Nous essayons d'utiliser notre propre compte ou mot de passe.

Il vaut la peine de noter que vous devez avoir une adresse e-mail vérifiée pour pouvoir vous enregistrer. Il n'y aura pas de rapport fait pour des abus anonymes. Si vous soumettez ce rapport d'utilisation malveillante et que le fournisseur ou le bureau d'enregistrement doit avoir plus d'informations, il doit pouvoir vous contacter pour avoir ces données.

Il y a aussi des webinaires et souvent, ces rapports sont utilisés pour retirer des compétiteurs sur l'Internet, etc. S'il y a une adresse e-mail, c'est assez complet, cela aide au niveau de la redevabilité de la personne qui fait le rapport. Nous, en tant qu'opérateur de NetBeacon, nous pouvons faire note de qui fait

une demande, etc. On peut ainsi limiter l'accès et restreindre les rapports d'utilisation malveillante qui passent par ce site.

Nous avons la prochaine page. Je vais agrandir un petit peu la page pour que vous puissiez voir ce que nous avons sur cette page et que vous puissiez la lire. Ce sera un petit peu brouillé parce que comme nous sommes en train d'enregistrer et cela complique les choses.

C'est un formulaire assez simple et là, nous allons indiquer l'URL du nom de domaine dont nous allons faire rapport. Par exemple, aujourd'hui, j'ai reçu une tentative d'hameçonnage et je vais indiquer le site avec l'URL. Voilà ce que je reçois en retour : je reçois un texto sur mon téléphone qui dit « La RBC a un message important : allez sur ce site netbeacon.org. » La Banque Royale du Canada est une banque importante au Canada. Je connais cette banque, mais je ne suis pas forcément un client. Pour moi, je sais que c'est un cas d'hameçonnage parce que je ne suis pas client de la RBC.

Je fais une capture d'écran de ce texto puisqu'il contient le nom de domaine et ensuite, je fais une capture d'écran de la page. Vous voyez la page de la RBC, mon compte a été suspendu, etc. Bien sûr, de suite, je me rends compte qu'il s'agit d'un cas d'hameçonnage.

Une note : il faut faire très attention pour résoudre ces URL parce qu'en général, il ne faut pas se diriger vers ces URL, il faut laisser cela aux professionnels. Cette capture d'écran avec ce nom de domaine devrait suffire.

Maintenant, j'ai le nom de domaine avec la RBC et je vais l'indiquer dans cette case. Ensuite, je clique sur « Continuer » et je vois que cela a été enregistré avec Tucows. Tucows a, bien sûr, réagi à ce rapport d'abus dès le départ. Maintenant, je peux choisir le rapport que j'ai fait. On peut avoir une approche avec plusieurs questions pour que ce soit plus facile à utiliser pour les utilisateurs finaux. Il faut rendre les choses les plus simples possible. On essaie de demander à la personne qui fait le rapport d'indiquer le genre d'utilisation malveillante dont il s'agit. La plupart des choses que l'on voit maintenant sont suffisantes. Ces informations sont [inaudible] souvent. Il s'agit de malwares et de spams.

Lorsque l'on clique sur le rapport que l'on fait, on va vous demander quel genre d'informations sont nécessaires et quelles informations sont utiles. Il est important de savoir que sans les bonnes données, un bureau d'enregistrement ne pourra pas agir sur ce rapport d'utilisation malveillante. Soumettre ce rapport sans ces informations ne compte pas car ces rapports, pour qu'ils soient gérés, doivent être complets. Si un bureau d'enregistrement reçoit un rapport sur lequel il ne peut pas agir,

il ne pourra rien faire. Nous devons nous assurer que tous les rapports soumis contiennent le plus d'informations possible.

Ceci nous amène à un nouveau formulaire, un rapport d'abus d'hameçonnage pour [inaudible]. On rentre dans le détail. C'était quand ? On peut dire aujourd'hui même si j'utilise un incident qui s'est déjà produit. Ensuite, qui était ciblé : la Royal Bank of Canada, la Banque royale du Canada. Je ne connais pas exactement le nom de domaine, mais on va mettre cela comme exemple.

Je reviens un peu en arrière, j'ai oublié quelque chose. Ce qu'on essaie de mettre ici, c'est des informations pour le bureau d'enregistrement qui a été usurpé dans cette tentative d'hameçonnage. Ce n'est pas moi, c'est la Banque Royale du Canada. S'il y a une connexion Apple, vous allez mettre Apple. Parfois, c'est évident si c'est une marque qu'on connaît. Tucows saura qui est la Banque Royale du Canada. Mais cela aurait pu être un bureau d'enregistrement en France qui ne connaît pas la Banque Royale du Canada ; donc il faut les aider à comprendre qui est ciblé par ce hameçonnage parce que ceci peut leur être utile.

Là, nous allons indiquer une brève description du problème. Dans ce cas, j'ai reçu un SMS d'hameçonnage pour la Banque Royale du Canada. Je pense que ceci suffit. Ce n'est pas

forcément facile de savoir quoi dire. Le bureau d'enregistrement a besoin de faits assez simples pour pouvoir couvrir autant de problèmes que possible.

Là, vous avez des fichiers que vous pouvez mettre. Là, je peux mettre mes captures d'écran. Je continue. Je peux sauvegarder ceci à n'importe quel moment de manière à pouvoir revenir à mon rapport de signalement. Si tout n'est pas prêt, vous pouvez sauvegarder et y revenir plus tard.

Nous demandons également le lieu. Pourquoi ? Parce que parfois, certains délits n'existent que dans certaines géographies sur la base de l'adresse IP. Ou alors, ce peut être une question de navigateur de l'utilisateur. À moins d'être sur un téléphone portable avec une adresse géographique précise, on ne peut pas voir quelle est l'attaque. Donc, il faut que le bureau d'enregistrement puisse savoir où cela se passe. Je vais mettre où je suis. Parfois, je peux demander à Siri de remplir automatiquement.

Si l'hameçonnage vient d'un e-mail, on peut mettre l'adresse de l'expéditeur. Dans ce cas, il ne s'agit pas d'un e-mail. Nous avons également de la place pour mettre le corps du message si encore une fois ce hameçonnage était effectué par e-mail.

Il faut noter que signaler un abus qui n'est que dans un e-mail et qui n'est pas passé par un site Web, il faut absolument mettre

les informations de l'e-mail. Il faut aller dans « View Email Source », voir la source de l'e-mail, voir l'original, et là vous allez avoir tout un tas de codes qui vont apparaître. Ces codes sont très importants pour les bureaux d'enregistrement afin qu'ils puissent savoir exactement qui a envoyé l'e-mail. Et lorsqu'ils regarderont dans le corps du message, ils comprendront ce qui est impliqué dans ce hameçonnage. C'est donc très important d'inclure ces informations si l'abus vient d'un e-mail. Mais ce n'est pas le cas ici.

Voilà, c'est tout. Vous envoyez ce rapport d'abus au bureau d'enregistrement. Les captures d'écran ne sont pas nécessairement incluses, mais NetBeacon va essayer d'obtenir ces captures d'écran et il va essayer d'obtenir le nom de domaine. Il va vérifier par rapport à d'autres sources d'information sur les abus, par exemple la navigation sécurisée de Google, il y a également les listes de blocage. Si les accès ont été donnés, on va vérifier d'autres informations par rapport à ce que vous avez envoyé. L'idée, c'est d'envoyer au bureau d'enregistrement autant d'informations que possible.

En termes de [inaudible], il faut absolument que je vous dise que Netbeacon a été mis en place par CleanDNS qui a donné leur technologie sous-jacente – et c'était dans leurs services – et ils ont donné aussi du temps pour personnaliser ceci. Je les

remercie donc. Voilà comment vous signalez un cas d'hameçonnage. Revenons à signaler un abus.

Si je reviens, je peux signaler d'autres incidents qui sont similaires. Vous allez de la même manière mettre le nom de domaine, vous allez sélectionner le type d'abus et vous allez suivre ce formulaire. Programme malveillant : il nous faut le nom de fichier où cela s'est passé. Même chose : capture d'écran, lieu. Si vous avez le programme malveillant MD5, toutes ces signatures de fichiers de programmes malveillants sont utiles, mais la plupart des gens n'ont pas accès à ce type d'information. Je pense que vous comprenez.

Ce formulaire est assez facile à utiliser. Il est relativement évident sans avoir à comprendre comment localiser le bureau d'enregistrement ou l'opérateur de registre pour envoyer le signalement.

Quelques petites notes quand même. Actuellement, nous ne travaillons qu'avec des opérateurs de registre génériques. On peut envoyer les abus à tous. Tous doivent avoir un contact en cas d'abus. Ils n'ont pas besoin de s'inscrire. On peut signaler à tout le monde et pour l'instant, ça va très bien.

Les bureaux d'enregistrement ont davantage de fonctionnalités. Ils peuvent créer des comptes spéciaux dans NetBeacon pour adapter leur réception des rapports.

Nous travaillons à l'intégration des ccTLD et c'est compliqué car les ccTLD sont tous différents d'une manière ou d'une autre, mais j'espère qu'on pourra les intégrer au cours des quelques mois à venir. Nous allons commencer par les plus grands, les plus faciles à gérer, et ensuite, on descendra dans la liste.

Est-ce qu'il y a d'autres choses à vous montrer ? Je peux peut-être vous montrer qu'il y a des réglages. Je peux changer mon identité, j'ai été vérifié, vous pouvez demander cette vérification. Demander la vérification, c'est pour ceux qui signalent un abus et qui le font, je ne sais pas si on peut dire professionnellement, c'est peut-être trop fort, mais qui le font assez régulièrement et qui ont certaines compétences.

Si vous demandez la vérification, vous allez avoir accès à des réglages qui vous donnent accès aux rapports sortants. Vous pourrez inclure le nom de votre organisation dans le titre du rapport enregistré. On saura d'où cela vient de manière plus évidente et cela vous permet également d'inclure un texte type au début à chaque fois. Peut-être que vous êtes un organisme de sécurité, donc vous mettez le nom de votre organisation en haut et dans le titre du rapport, vous pourrez dire « Voici notre organisation, voici notre site Web, voici nos coordonnées si vous avez besoin de nous contacter. » Cette fonctionnalité, c'est pour ceux qui demandent la vérification dans les réglages.

Et puis, il y a une API. Encore une fois, si vous faites ceci souvent, si vous avez les compétences nécessaires, vous pouvez envoyer des rapports d'abus directement dans l'API de NetBeacon.

Voilà, je crois que c'est tout ce que je souhaitais vous démontrer ici aujourd'hui. Je suis prêt à écouter votre feedback. Je n'ai pas suivi toutes les questions qui ont été mises dans le chat, mais peut-être ce que je peux faire, c'est d'arrêter de partager mon écran et nous pouvons répondre à ces questions.

OLIVIER CRÉPIN-LEBLOND : Merci beaucoup, Graeme. Je ne sais pas si vous souhaitez modérer, Jonathan.

JONATHAN ZUCK : Est-ce que vous m'entendez maintenant ?

OLIVIER CRÉPIN-LEBLOND : Oui, allez-y, vous pouvez gérer la partie questions et réponses.

JONATHAN ZUCK : Très bien.

Une petite question rapide pour vous, Graeme. Pour faire cette démonstration, vous avez utilisé un ancien rapport, je crois. Si l'un d'entre nous souhaitait faire la démonstration à quelqu'un

d'autre, est-ce que vous avez une suggestion pour le faire de manière qu'on n'envoie pas un rapport en double ? Comment-peut-on faire une démonstration ? Est-ce que vous avez un faux-rapport que vous utilisez pour les démonstrations ? Quelle est la meilleure manière de le faire pour nous ?

GRAEME BUNTON : Très bien. Je suis prêt à faire cette démonstration. Vous n'avez pas à le faire, mais c'est très bien si vous le souhaitez.

Le plus simple, c'est de prendre un spam, un pourriel dans votre fichier de spams. J'imagine que tous, vous en avez. C'est un petit peu moins intéressant que l'hameçonnage et c'est une des raisons pour lesquelles je n'ai pas utilisé un e-mail aujourd'hui, mais prenez un pourriel comme exemple. Il y a quand même un petit bémol : beaucoup de pourriels viennent de Google, d'adresse Gmail. Faire un signalement au bureau d'enregistrement Gmail, je crois que c'est [inaudible], ce n'est pas forcément la meilleure manière. On ne va pas éliminer Gmail.com. Prendre peut-être un pourriel qui ne vient pas de Gmail ou qui ne vient pas d'un grand fournisseur de services de courriel, c'est sans doute une bonne idée.

JONATHAN ZUCK : Je ferai peut-être un suivi là-dessus avec vous. Ce serait bien, je trouve, d'avoir un plan pour faire une présentation à un niveau un petit peu plus bas de la structure, pour les ALS peut-être, leur faire une démonstration. Il serait bon de pouvoir mettre ceci en place, mais on pourra en parler tous les deux après.

Sébastien Bachollet, vous avez une question, allez-y.

SÉBASTIEN BACHOLLET : Merci beaucoup, Jonathan. Merci pour la présentation, Graeme. J'ai une question.

J'ai essayé d'expliquer aux gens ce qui se passe lorsqu'ils reçoivent un SMS. Ne touchez pas le lien, ne faites rien. Cela veut dire que vous dites l'inverse, vous dites « Allez-y, mettez les informations dans NetBeacon. » Comment pouvons-nous, en tant qu'utilisateurs finaux, envoyer directement un SMS quelque part pour nous occuper de cette question ? Parce que d'une manière générale, il me semble que même si on essaie de rendre les choses pas compliquées, c'est quand même compliqué pour l'utilisateur lambda et ce sera donc trop compliqué, je crois. En fait, il n'y a que les spécialistes qui pourront le faire et les autres ne feront rien par rapport à cette question de l'utilisation malveillante du DNS.

Merci.

GRAEME BUNTON : Je ne peux pas dire le contraire. Oui, ne cliquez sur rien, vous avez raison, n'allez pas sur cet URL. Il devrait être assez sécurisé de faire une capture d'écran du SMS. Cela devrait aller. J'ai inclus la capture d'écran du site Web parce que je sais ce que je fais dans ce cas-là, et c'était pour aider les gens à comprendre. En fait, c'est vrai, il faut absolument dire aux gens de ne pas cliquer sur ces liens. C'est une mauvaise chose à faire. Télécharger cette capture d'écran, c'est tout à fait sécurisé.

Nous manquons de capacités pour certains services, bien sûr, mais nous essayons de faire cela pour les courriels. Si vous recevez un courriel d'hameçonnage ou un pourriel, vous pouvez faire passer cela à NetBeacon. Ils vous diront d'envoyer cela vers les bureaux d'enregistrement. La chose difficile, c'est qu'on ne peut pas renvoyer un courriel, on doit l'envoyer en tant que pièce jointe. C'est assez simple dans ce sens.

Je vois qu'il y a une main levée de la part d'Amrita.

AMRITA CHOUDHURY : Je pense que c'est une très bonne initiative, Graeme. C'est un bon moyen de commencer parce que cela pose vraiment problèmes. Mais il y a deux questions. Quand vous vous enregistrez sur le système, il faut une adresse e-mail. Dans

beaucoup de pays, ils n'ont que des mobiles et les gens n'ont pas ce genre de choses, donc il faut s'occuper de cela.

Une autre question, vous en avez parlé d'ailleurs : comment les utilisateurs peuvent différencier les différents types d'utilisation malveillante ? Aussi, la plupart des gens ne sont pas capables de faire cela, ils ne sauront pas comment signaler ces choses. Ils savent que c'est une utilisation malveillante, mais ils ne savent pas quelle sorte d'utilisation malveillante. Ils ne vont pas tout lire.

Merci.

GRAEME BUNTON : Merci Amrita. Je vais en parler simplement.

À mon avis, il y aura toujours des obstacles techniques pour faire ces signalisations d'utilisation malveillante. J'aimerais simplifier cela le plus possible, mais en fait, cela demande tout de même une sorte de compétence, une sorte d'expertise pour faire ce genre de rapport de signalisation. Oui, j'aimerais bien arriver à un moment où on pourrait prendre n'importe quelle sorte de domaines de domaines et dire : « C'est du hameçonnage, c'est du pourriel, etc. », mais on est loin de cela ; pour l'instant, il nous reste encore beaucoup de travail à faire.

En attendant, je pense qu'il y a tout de même encore un petit obstacle. C'est désolant. Mais nous continuerons à travailler.

Je pense qu'il y a une question sur le chat de la part de Naveed. Il parle de numéros de téléphone. Nous n'avons pas considéré cela pour l'instant. Je vais devoir y penser, à savoir si on peut utiliser ces numéros de téléphone. Pour l'instant, nous utilisons les adresses courriel. J'ai d'ailleurs sur ce sujet un document avec beaucoup d'informations sur les choses qu'il nous reste à faire. Je prendrai toutes ces notes en considération.

JONATHAN ZUCK : Siva.

SIVASUBRAMANIAN MUTHUSAMY : Même avec les gens qui ont des expertises techniques, les classifications de ce genre d'utilisation malveillante, c'est un facteur qui limite les utilisateurs. Moi, j'ai fait l'expérience d'un incident il y a peu de temps qui ne pourrait pas être classifié en tant qu'hameçonnage même si cela contenait des éléments de preuve d'utilisation malveillante. Il y avait l'élément de malware dans l'aspect de conception de cette utilisation malveillante, mais c'était difficile de choisir la catégorie. Est-ce qu'il serait possible d'avoir une autre catégorie pour les personnes qui ne savent pas comment classifier cette

utilisation malveillante ? Parce que tous les utilisateurs n'ont pas forcément la compétence de le faire.

GRAEME BUNTON : Je pense que ce n'est pas aussi simple, malheureusement, pour identifier ces utilisations malveillantes. Mais nous allons le considérer.

En général, sachez que ce système est assez nouveau. Nous avons commencé en juin l'année dernière. Nous apprenons encore et nous allons voir s'il y a des moyens de modifier cette interface, si elle peut s'améliorer. Je pense qu'avec le temps, nous allons pouvoir améliorer ce système. Il y a beaucoup de travail en cours. J'aime beaucoup ces retours d'information pour pouvoir, justement, améliorer ce service. Ce peut être un service qui peut être bon pour le public. Nous savons très bien qu'il n'est pas parfait pour l'instant ; c'est pour cela que toutes ces informations sont très utiles.

Je vois qu'il y a une question dans le chat à savoir si les gens sont informés de la suite des évènements. Pour l'instant, la réponse est non. Nous essayons de mettre en place un système de surveillance pour faire le suivi. Est-ce que le nom du serveur a changé ? Est-ce que le site a changé ? Est-ce que les enregistrements ont changé ? Est-ce que le contenu de la page signalé a changé ? C'est pour savoir si ces dommages ont été

atténués ou pas. Il pourrait s'agir du bureau d'enregistrement de l'utilisateur malveillant qui était la cause de cette utilisation malveillante.

La bonne réponse pour atténuer cette utilisation malveillante, ce n'est pas forcément de retirer le site. Il peut y avoir un problème sur le site, un site compromis, etc. Arrêter ou retirer ce DNS ne sera pas forcément approprié. Encore une fois, ce ne sera peut-être pas forcément la bonne chose à faire. Il y a d'autres genres d'atténuation.

Marita a la main levée.

MARITA MOLL : Bonjour Graeme. Je pense que c'est une très bonne initiative. Je ne pense pas que ceci ait l'air trop compliqué, mais ce qu'il nous faut, c'est informer et éduquer les gens éduquer parce que pendant des années, aucune agence n'a voulu faire face à ce genre de choses. Personne n'avait de moyens pour signaliser ces abus. C'est donc un bon commencement, à savoir que maintenant on sait qu'on peut faire quelque chose et qu'on a une façon de le faire.

Nous avons à travers toutes nos chaînes variées essayé de trouver des moyens d'éduquer les personnes sur les impacts potentiels de ce genre de service, à savoir comment cela peut

être signalé, comment on peut améliorer les choses. Que puis-je dire de plus ?

GRAEME BUNTON : Merci Marita. Donc, nous continuons à travailler sur ce sujet.

Je vois qu'il y a une question dans le chat de Dave qui nous parle de la signalisation de l'URL au complet. C'est beaucoup plus utile parce que c'est là qu'on peut absolument signaliser le cas d'abus à la source du nom de domaine.

Attendez, je ne vois pas, ça va trop vite dans le chat.

Au niveau des statistiques par rapport à ce que l'on gère, nous avons des statistiques. Nous mesurons cela par milliers par mois, c'est important. Le site est bien utilisé. Nous ne publions pas ces données sur netbeacon.com parce que nous voulons que les bureaux d'enregistrement et tous ces groupes puissent participer sur NetBeacon et nous aider à augmenter ce lien.

Il y a un autre projet qui s'appelle DNSAI Compass pour mesurer le DNS à travers tout l'écosystème, les ccTLD, les gTLD et les bureaux d'enregistrement. Cela signale un rapport agrégé de l'utilisation malveillante. On a commencé au mois de septembre. Vous pouvez trouver ces informations si vous faites une recherche Google DNSAI Compass.

Nous allons continuer à publier des rapports de l'utilisation malveillante. Nous inclurons les bureaux d'enregistrement et les TLD qui ont un taux d'abus un peu plus bas. Nous voulons être rigoureux et transparents et nous voulons avoir une approche académique vis-à-vis de cet écosystème d'utilisation malveillante. Cela nous aidera vraiment à comprendre l'échelle de ces abus.

Je vois qu'il y a une autre main levée.

OLIVIER CRÉPIN-LEBLOND : Deux questions rapides.

Tout d'abord, quand il s'agit du langage utilisé, est-ce que vous allez étendre ce service vers d'autres langues ? Parce que pour l'instant, il ne s'agit que de l'anglais.

Aussi, comment allez-vous gérer les requêtes faites pour les tous les domaines ?

GRAEME BUNTON : Nous voulions le faire en anglais en premier pour savoir comment les personnes allaient utiliser ce service et pour pouvoir en apprendre un peu plus avant d'avoir passé à l'étape de traduction de tout cela.

Tout d'abord, les codes géographiques, cela va venir la plupart du temps. Dans ce cas, les abus sont liés aux bureaux d'enregistrement puisque ce sont eux qui sont responsables. Quant aux TLD, il y a des informations dans les entrées WHOIS qui nous rendent la vie un peu plus difficile. Par exemple, cela ne fournit pas de données de bureaux d'enregistrement, donc il est impossible d'envoyer leurs rapports de la bonne manière, du moins pour nous.

Ce que nous voulons faire pour les TLD comme cela, c'est de les envoyer directement vers les opérateurs de registre et leur demander de distribuer ces données directement pour nous. Pour les autres, c'est OK si nous pouvons identifier le bureau d'enregistrement, si c'est un bureau d'enregistrement qui est déjà accrédité par l'ICANN parce que cela centralise tous les rapports d'abus directement au bureau d'enregistrement. C'est un peu plus compliqué pour les [ccTLD], mais nous allons essayer de centraliser toutes les données.

OLIVIER CRÉPIN-LEBLOND : Si quelqu'un soumet un rapport, est-ce que le système va notifier ces gens-là et signaliser cela ? On va leur dire « Allez-y » ou « Ne l'acceptez-pas » ?

GRAEME BUNTON : Non, ce ne devrait pas pouvoir être accepté. Il y aura une erreur qui va survenir et on va nous dire que le TLD est signalisé.

OLIVIER CRÉPIN-LEBLOND : Je pense que c'est important. Beaucoup de membres ne connaissent pas la différence. Il y a des ccTLD qui prétendent être des gTLD et il y a des gTLD qui prétendent être des ccTLD pour tout le monde.

GRAEME BUNTON : Oui, bien sûr, je suis d'accord. On se dit : est-ce qu'on peut mettre en place le système ? Est-ce que l'on peut s'assurer que cela fonctionne pour que ce soit utile pour tout le monde ? Bien sûr, nous voulions que ce soit utile. Au niveau des domaines et des gTLD, nous voulions commencer par cela. Nous savons qu'il y a beaucoup plus d'éléments qui sont pertinents à cette catégorie générique.

Le problème avec cette signalisation d'abus en ce moment, c'est que beaucoup d'opérateurs de registre et de bureaux d'enregistrement reçoivent ces signalements par courriel sans pouvoir catégoriser comme nous le faisons. On a mis en place ces catégories différentes. Nous savons que les personnes vont pouvoir choisir. Si on ne fait pas cela, on ne va pas avoir une qualité de signalisation suffisante. On veut faire un meilleur

travail sur cette interface pour les utilisateurs. On veut aider pour essayer d'atténuer ces signalisations en utilisant ces catégories pour pouvoir justement limiter les données.

Je vois qu'il y a une main levée de Siva.

SIVASUBRAMANIAN MUTHUSAMY : Une observation.

Après avoir soumis le rapport, est-ce qu'il y a une possibilité pour la personne qui fait le rapport d'obtenir un rapport additionnel avec des informations ? Je ne vois pas cela sur votre interface. En plus, comme on l'a dit dans le chat, est-ce que ceci se passe sur tout ce qui est en matière d'abus ? Pourquoi ne parle-t-on pas aux opérateurs de registre ?

GRAEME BUNTON : On ne peut pas changer le rapport fait parce qu'on doit envoyer toutes les informations au départ quand on soumet ce rapport d'utilisation malveillante. Un des problèmes pour les bureaux d'enregistrement, c'est qu'il y a un renvoi des rapports. Après, on rentre dans des moyens d'incompréhension. Cela devient compliqué.

Quand ces rapports vont vers les bureaux d'enregistrement, ces rapports contiennent vos informations. L'adresse d'envoi est NetBeacon, mais il y a aussi vos informations. Si le bureau

d'enregistrement a besoin de plus d'informations, il peut vous contacter directement pour qu'on ne soit pas au milieu de la communication.

Quand il s'agit des opérateurs ou des bureaux d'enregistrement, dans la plupart des cas, sachez que le bureau d'enregistrement a la relation avec les utilisateurs. Les utilisateurs, c'est une relation avec le bureau d'enregistrement. Donc, pour la plupart des utilisateurs, quand il s'agit pour eux de déterminer s'il y a un abus, le bureau d'enregistrement est plus proche du problème et il peut mieux comprendre.

Dans certaines circonstances, lorsqu'il s'agit des réseaux zombies, si le nom n'est pas encore enregistré, il faut essayer de voir où il y a une possibilité d'aller vers l'opérateur de registre. Mais dans la plupart des cas, les bureaux d'enregistrement sont responsables pour les cas d'utilisation malveillante.

SIVASUBRAMANIAN MUTHUSAMY : Il y a cinq ou six ans, on parlait d'utilisation malveillante du DNS à l'ICANN durant les forums. On parlait des enregistrements officiels et on parlait du nombre d'utilisations malveillantes signalisées et on parlait de 10 à 20 millions. Ce chiffre a été signalé et enregistré comme cela. Maintenant, on pourrait en être à plus.

Cette approche simplifiée de signalisation va simplifier le processus. Vous pensez que le nombre d'incidents reliés aux abus serait plus négligeable ?

GRAEME BUNTON : Merci, bonne question.

J'ai beaucoup travaillé là-dessus dans le cadre du projet Compass qui mesure les abus. On a mesuré les programmes malveillants et l'hameçonnage parce que c'est là que nous avons le plus de données. En général, il s'agit de la consommation de liste de blocage avec l'agrégation, la duplication de tickets, etc.

L'ICANN a un projet qu'ils appellent le DAAR, le système de signalement des cas d'utilisation malveillante, qui est relativement bon avec beaucoup de données. Mais c'est assez technique comme travail. Selon leurs estimations avec plusieurs sources, plus de sources finalement que ce que nous avons utilisé dans le cadre du Compass, selon eux, il y aurait 650 000 noms de domaine abusés en un mois. Je parle de pourriels, d'hameçonnage et de réseaux zombie. Sur le nombre total de noms de domaine, 260 millions, ce 650 000, vous voyez donc que dans tout le DNS, c'est en fait une toute petite fraction des noms de domaine qui sont abusés. Même pour des listes qui sont courtes, elles ne sont pas suffisamment signalées. Il y a des listes

qui ne contiennent pas tout. Même si on multiplie ce chiffre par deux, c'est moins de 1 sur 260 noms abusés. Donc, le chiffre est assez bas.

Marita.

MARITA MOLL : Merci de m'écouter. Vous êtes Canadien, moi aussi, donc je vais parler du .ca.

Si je signale le .ca, qu'est-ce qui se passe ?

GRAEME BUNTON : Il n'y a pas d'abus au Canada. Malheureusement, le .ca, nous y travaillons. Nous n'avons pas encore avancé là-dessus. Je suis en contact avec les gens du .ca pour voir si nous pouvons travailler ensemble.

Je pense que c'est un problème de mon côté pour obtenir les sources de données, la connectivité. Très honnêtement, nos priorités pour les ccTLD, c'est les plus grands et ceux qui sont le plus affectés parce qu'on pourra signaler davantage aux bureaux d'enregistrement. Le .ca est déjà grand, mais il faut dire qu'en fait c'est une bonne zone qui n'est pas vraiment affectée. Bien sûr que j'aimerais personnellement qu'on y arrive, mais ce n'est pas la priorité pour l'instant.

JONATHAN ZUCK : Merci beaucoup, Graeme, d'avoir pris le temps pendant vos vacances professionnelles à Barcelone.

MICHAEL PALAGE : J'ai une question pour Graeme, si je peux me permettre, Jonathan.

JONATHAN ZUCK : Oui, on avait dit que c'était terminé, mais allez-y.

MICHAEL PALAGE : Graeme, rapidement, par rapport aux mesures de rapport de PIR, j'ai vu que vous avez fait le détail de tout ce qui a été retiré par les agences d'application de la loi, les réseaux zombies, etc. Est-ce qu'il y a des situations autres où vous avez une catégorie attrape-tout pour certains contenus ? Ma question, c'est lorsque que PIR élimine un nom de domaine, est-ce que tout ceci est signalé ? Ou alors, est-ce que parfois certaines éliminations ne sont pas signalées ?

GRAEME BUNTON : Merci Michael.

Honnêtement, je n'en ai aucune idée. L'Institut, moi-même, nous travaillons totalement à l'externe. Donc, on se concentre sur tout l'écosystème du DNS et je ne considère pas l'abus PIR interne, je ne m'occupe pas de leurs rapports d'abus, je ne gère pas leurs signalements. Parfois, cela passe par NetBeacon, on mesure par Compass. Mais le .org et les autres abus payeurs, tout ceci passe par Brian Cimbolic. Je ne le vois pas. Ceci est important pour la crédibilité de l'Institut parce qu'il faut pouvoir travailler dans tout l'écosystème. Et être intégré avec PIR, cela créerait un conflit d'intérêts. En fait, je ne vois pas tout cela.

MICHAEL PALAGE : Oui, je comprends bien et je ferai le suivi avec Brian là-dessus parce que je crois que c'est une meilleure pratique. [inaudible] Digital a le même détail. En tout cas, merci pour cette réponse.

GRAEME BUNTON : Merci. Je mettrai mon adresse e-mail dans le chat. Si vous souhaitez me contacter, si vous avez d'autres questions, si vous voulez une autre démonstration, si vous avez découvert un problème et que vous avez un feedback, n'hésitez pas, je suis très ouvert. Je serai en contact avec Jonathan pour lancer le programme Compass avec le rapport détaillé parce que je pense que ce sera très intéressant.

JONATHAN ZUCK : Très bien, cela me semble prometteur. Merci encore.

Olivier.

OLIVIER CRÉPIN-LEBLOND : Merci beaucoup, Jonathan.

Merci Graeme d'avoir présenté cet outil. Je suis toujours ravi de vous inviter à ces appels pour nous parler un peu du DNS. Beaucoup de gens parlent, mais il n'y en a pas beaucoup qui font quoi que ce soit sur l'utilisation malveillante du DNS. Il y en a, mais je crois que le DNS Abuse Institute a énormément contribué, surtout du point de vue des utilisateurs finaux et ceci est apprécié.

Nous passons maintenant à la suite avec les mises à jour des petites équipes. Cette semaine, pas de mises à jour sur le PDP TPR.

La première mise à jour porte sur le processus d'élaboration de politiques accéléré sur les noms de domaines internationalisés. Nous allons donc céder la parole à Hadia El Miniawi ou peut-être Justine. Je ne sais pas exactement qui va faire la présentation. C'est Justine, très bien. Alors, Justine Chew, c'est à vous.

JUSTINE CHEW : Merci Olivier. Est-ce que j'ai 15 minutes ou est-ce que c'est moins ?

OLIVIER CRÉPIN-LEBLOND : Vous avez 15 minutes.

JUSTINE CHEW : Très bien. Je vais procéder de manière judicieuse parce qu'il y a deux semaines, nous n'avons pas pu tout faire. Donc, je me suis dit que je vais procéder différemment et je vais présenter toutes les diapositives. S'il y a des questions, n'hésitez pas à les poser dans le chat et je demanderai à Satish de gérer le chat et de répondre autant que possible. Si on ne répond pas à toutes vos questions aujourd'hui, nous enregistrerons vos questions et nous reviendrons vers vous par la suite.

Il y a deux sujets qui nous intéressent aujourd'hui : la révision de la similitude des chaînes et les conflits de chaînes. Je ne parlerai certainement pas des autres sections dont nous avons déjà parlé il y a deux semaines, mais on y reviendra la semaine prochaine. Il y a plusieurs ressources à la fin de la présentation, vous pouvez donc aller voir après. Diapositive suivante, s'il vous plaît.

Nous avons déjà beaucoup parlé de ceci lors du rapport initial. Ce qui est en jaune, nous l'avons déjà mentionné. Pour le 4.3, j'ai

uniquement surligné le chiffre parce que pour ce point, nous avons essayé de terminer cela il y a deux semaines mais nous n'avons pas réussi. Aujourd'hui, je vais parler de la révision de similitude de chaînes et du conflit de chaînes, comme je le disais tout à l'heure. Diapositive suivante.

Nous avons déjà parlé du fait qu'on utilise la règle de génération d'étiquettes pour la zone racine comme source unique pour déterminer les étiquettes des domaines de premier niveau valides. Vous voyez le récapitulatif, j'imagine que vous le connaissez déjà, nous en avons déjà parlé.

Si je regarde à gauche la légende, ce que vous avez en jaune, c'est l'étiquette de source primaire. C'est ce que l'on met dans l'outil, le RZ-LGR 2, qui correspond à l'ensemble d'étiquettes. C'est le tableau de l'ensemble des étiquettes et vous avez différentes valeurs de dispositions qui sont allouables en bloc. Qu'est-ce que cela veut dire ? Allouable, c'est qu'on peut déléguer et qu'on peut affecter. Bloquer, il n'y a pas de possibilité d'allouer ou d'affecter. Je ne vais pas passer par tout le processus de remise en cause de tout ceci parce que c'est une autre question.

Je récapitule pour que vous puissiez comprendre. Vous avez l'ensemble d'étiquettes primaires allouables, vous avez « bloqué » et « allouable ». L'étiquette de variante dépend de

l'étiquette primaire ; voilà pourquoi il faut d'abord déterminer l'étiquette primaire avant de déterminer l'ensemble des étiquettes de variantes.

Ensuite, en termes de similitudes de chaînes et de sa révision, lors de la série de 2012, nous avons utilisé ce qu'on appelle le test visuel. Que se passe-t-il lorsqu'il y a un panel de révision de similitude de chaîne ? On prend deux chaînes et on essaie de voir visuellement s'il y a une similitude ou une possibilité de confusion, si elles sont suffisamment similaires pour que l'utilisateur se trompe entre les deux. C'est l'idée de ce test. Ce qu'on fait, c'est qu'on compare les étiquettes dans le même script ou entre les scripts, entre les alphabets parfois, surtout lorsque les chaînes sont faciles à confondre. Par exemple, lorsqu'on a « aaa », vous voyez les trois « a » en alphabet latin qui sont tout à fait similaires aux trois « a » en alphabet cyrillique.

La révision de similitude de chaînes a lieu avant l'objection. Tout ce qui n'est pas repéré par cette révision de similitude peut être interrompu dans le processus d'objection. C'est pour la série de 2012.

Dans le graphique, ce que vous avez ici, c'est ce qui se passe lorsqu'on commence à introduire des variantes et quel est leur rôle dans cette révision de similitudes de chaîne. L'équipe EPDP

a rassemblé une petite équipe pour réfléchir à cette question précise et cette petite équipe a émis certaines recommandations au bout d'un certain temps. Je me souviens que j'avais fait cette présentation en octobre 2022, donc je ne vais pas revenir sur tous ces détails. Je vais essayer de rester à un niveau très conceptuel pour expliquer.

Lorsqu'on parle du niveau 1, du niveau 2 et du niveau 3 sur ce diagramme, vous avez un petit peu ce à quoi cela correspond. Le niveau 1, c'est le niveau primaire et allouable qui correspond à une comparaison de similitude des chaînes. Le niveau 1, c'est primaire plus demande... Attendez un instant, je me suis trompé. Primaire plus variante demandée. Le niveau 2 : primaire plus toutes les variantes allouables, qu'on ne demande pas. Et le niveau 3, c'est tout. D'accord ? Y compris ce qui est bloqué.

L'idée, c'est que lorsqu'on introduit ces différents niveaux, la comparaison devient plus compliquée parce que vous avez augmenté le nombre d'étiquettes. Lorsqu'on en compare une, par exemple à gauche, vous avez une étiquette et à droite, vous en avez 10, donc vous comparez quelque chose 10 fois. D'accord ? Imaginez-vous un petit peu si à gauche vous en avez 100 et qu'à droite vous en avez 100. Là, cela devient en fait ingérable.

Dans ce contexte, nous en sommes arrivés à un point d'adaptation par rapport à une série de 2012 pour équilibrer la minimisation des complications. Nous voulions atténuer.

Si nous passons à la prochaine diapo, voilà un exemple qui n'est pas nouveau. Vous connaissez ces tableaux. Je voulais juste partager les informations sur la façon dont nous avons décidé d'utiliser le modèle hybride. Nous faisons une section croisée des trois niveaux dont j'ai parlé avec tout de même l'exception du fait que nous ne demandions pas une comparaison des variantes bloquées. Il n'y avait pas de variantes dans la série de 2012. C'est comme cela que nous avons terminé d'ailleurs avec cet EPDP.

À cette époque, nous ne comparions qu'A1 et B1. Nous avions deux étiquettes et nous comparions A1 et B1, c'était tout. C'était visuel. Si on voyait que l'un des deux était un TLD existant, l'autre ne pouvait pas continuer et n'était pas délégué encore. C'était simple.

Mais lorsque l'on a commencé à introduire des étiquettes de variantes et qu'on a commencé à augmenter le nombre de comparaisons, nous avions une nouvelle situation et là, nous avons commencé à utiliser ce modèle hybride. Il y a une raison pour cela. Avec ce modèle, pour les deux niveaux primaires, les deux étaient comparés l'un à l'autre, les deux étiquettes plus

importantes A et B. Mais maintenant, on doit aussi comparer B1 avec A2 et A3. On a commencé à introduire ces étiquettes de variantes. La boîte verte, c'est ce qui est alloué et tout ce qui est en rose est bloqué. Nous avons le groupe 1. A1 contre B1, nous avons B1 contre A2 et A3. C'est la racine 3. Ensuite, B1 contre A4 et A24. C'est un des contextes.

De l'autre côté, nous avons une situation croisée où nous avons A1, B2 et B23. A2 contre A3 et A3 contre B2 et B23. Nous avons des connexions. Nous avons vu que si nous n'introduisions pas ce niveau de comparaison, nous ne pourrions pas absolument déterminer quels sont les problèmes en jaune. En introduisant ce processus, nous pouvons ainsi déterminer les combinaisons d'étiquettes de similitude. Si nous n'avions pas introduit ces étiquettes de variantes dans ces comparaisons, nous ne pourrions pas en arriver à ces résultats.

La bonne chose dans tout cela, c'est que nous avons trouvé des étiquettes similaires et nous pouvons ainsi déterminer s'il y a des moyens de continuer ou de mettre cela dans des ensembles de [contention]. S'il y a des similitudes, dans ce cas-là, on ne pourrait pas déléguer et il y aurait confusion au niveau de l'utilisateur final. C'est pour cela que l'on a utilisé ce modèle hybride, parce que cela nous aide à déterminer et à pouvoir expliquer d'autres comparaisons et d'autres combinaisons d'étiquettes similaires, ce qui nous aide à détecter les

problèmes. Voilà comment ce modèle fonctionne. Nous passons à la prochaine diapo.

Nous essayons d'atténuer le problème en utilisant ce modèle hybride. Le problème, c'était le déni de service. Il y avait un manque de connexion et collectivement, il y avait un manque de détermination des erreurs. Cela posait un problème parce qu'on est envoyé à un endroit où quelqu'un peut vous causer des dommages. Donc, il y avait des risques de mauvaise connexion. D'ailleurs, comme vous le voyez, le diagramme est assez compliqué, mais en fait on essaie de démontrer cela. Si quelqu'un observe une étiquette verte comme on le voit ici et pense que cela est correct, si c'est incorrect, cette personne va se retrouver dans un endroit différent de ce à quoi il s'attendait. Il y a quand même un élément de confusion dans tout cela. On est dirigé de la mauvaise manière au mauvais endroit. C'est ce qu'on appelle une mauvaise connexion. Il y a toujours un risque d'abus dans ce cas-là, parce qu'on vous envoie et on vous dirige à un endroit où vous ne vouliez pas aller, un endroit auquel vous ne vouliez pas vous connecter. Cela causait de la confusion, de la frustration. Cela pouvait aussi compromettre vos données, vous exposer à des utilisations malveillantes. C'est là où vous pouvez avoir un abus du DNS.

On essaye de d'atténuer ceci en introduisant des variantes dans notre processus de révision pour essayer, justement, d'atténuer

ou de résoudre ces confusions afin qu'il n'y ait pas de délégations séparées ou de délégation du tout d'ailleurs avec ces chaînes similaires. On passe à la prochaine diapo.

J'ai essayé d'expliquer ceci auparavant, mais voilà l'effet de l'adaptation de la similarité des chaînes et de cette révision, de ce mécanisme de processus vis-à-vis de la série de 2012. Comme je l'ai déjà dit, cela requière une comparaison qui doit être faite à tous les niveaux de chaînes de caractères les uns par rapport aux autres, à l'exception de bloqué contre bloqué. Il s'agit d'atténuer les risques potentiels de déni de service et/ou de mauvaise connexion. D'ailleurs, ces deux risques sont toujours présents. Il faut aussi pouvoir détecter plus de combinaisons d'étiquettes visuellement confuses. Et ensuite, on ne demande pas des comparaisons de bloqué contre non bloqué, il faut éviter cette complexité inutile. Cela a été présenté à l'appel du CPWG le 10 octobre 2022. Nous n'avons pas reçu d'objection à ce moment-là.

Pour ce qui est de la recommandation vis-à-vis de ce modèle, maintenant, nous savons qu'il a été accepté en général. Il y a tout de même des exceptions, 4.2 et 4.3. Le 4.2 parle du fait qu'on pourrait permettre au [SSR] de décider quelles étiquettes de variantes bloquées doivent être omises dans le SSR.

La mission doit être fondée sur des lignes directrices, des critères sur la base d'un niveau manifestement faible de confusion entre les écritures, la recherche, les études supplémentaires pour identifier ces écritures. Mais essentiellement, les critères ou les lignes directrices que nous avons observés doivent être élaborés au cours de la mise en œuvre et on doit savoir ce que cela veut dire, bien sûr. Cela peut être expliqué simplement.

Si on compare des chaînes en langue latine contre les chaînes en script chinois par exemple, les scripts sont très différents, un avec l'alphabet et l'autre avec des idéogrammes. Il s'agit juste de formes d'idéogrammes. Il y a très peu de possibilités de combinaisons de lettres qui pourraient porter à confusion. C'est ce que l'on veut dire quand on parle de donner la flexibilité à ce panel pour déterminer comment on pourrait omettre des comparaisons redondantes qui ne sont pas nécessaires. Dans le cas que j'avais donné, il y a un peu de possibilités qu'une étiquette latine soit similaire à un script chinois, les combinaisons de scripts qui pourraient tomber sous un niveau assez bas de confusion.

Comme je l'ai dit tout à l'heure, la recommandation 4.3, les lignes directrices peuvent être élaborées au cours de la mise en œuvre.

La 4.4 est liée à l'intégrité d'un ensemble d'étiquettes de variantes dont on a parlé auparavant. Une fois que les ensembles de variantes ont été identifiés, ces ensembles doivent être conservés dans leur totalité pour préserver leur intégrité.

Que se passe-t-il pour ces étiquettes qui appartiennent à cet ensemble d'étiquettes ? Quel impact y aura-t-il par rapport à l'ensemble des étiquettes ? En fait, lorsque l'on fait cette candidature pour cet ensemble d'étiquettes de variantes, ceci sera comparé à des TLD qui sont déjà existants, à savoir s'il y a des similitudes pour cet ensemble pour être éligible à continuer si les deux groupes, qui peuvent être parfois similaires et non délégués, sont appliqués et c'est ce qu'on essaie de faire à la base.

OLIVIER CRÉPIN-LEBLOND : On vous demande, Justine, d'aller un peu plus vite parce que nous avons un temps un parti pour notre appel.

JUSTINE CHEW : Quand on regarde les 6.1 et 6.2, je pense que c'est assez clair. Je vais m'arrêter là.

OLIVIER CRÉPIN-LEBLOND : Je réalise que nous n'avons que très peu de temps. Je sais que 10 ou 15 minutes, ce n'est pas beaucoup de temps pour vous. Malheureusement, nous n'avons pas assez de temps aujourd'hui encore une fois et nous avons d'autres éléments à couvrir. Nous devons parler des mises à jour au niveau des politiques. Merci Justine pour votre mise à jour. Nous entendrons plus de détails sur le travail de votre groupe la semaine prochaine.

Maintenant, nous allons passer à Hadia.

SARAH KIDEN : Olivier, si je peux me permettre, nous avons également le processus de directives africain.

OLIVIER CRÉPIN-LEBLOND : Oui, j'avais oublié. Le processus de soutien aux candidats. Désolé, Maureen, je me suis trompé étant donné les limites de temps.

SARAH KIDEN : Pas de problème Olivier, très brièvement. Maureen n'est pas avec moi, donc je vais faire cette mise à jour.

Je ne sais pas si vous vous souvenez, mais en novembre 2022, nous avons commencé notre travail avec le GGP et nous avions six tâches à effectuer. Nous avons terminé les tâches 1 à 5 et

nous sommes en train de sur travailler la dernière tâche, la tâche 6. Vous pouvez consulter la diapositive par la suite. Passons à la suivante.

À la base, la tâche 6 a pour objectif de recommander une méthodologie d'allocation de soutien financier où il y a un financement inadéquat pour des candidats qualifiés. L'idée, c'est que s'il y a 10 candidats qui sont soutenus dans le cadre du programme, on pourra considérer que c'est une réussite.

Mais que se passe-t-il si le programme en reçoit 15 ou 20 qui sont qualifiés et qui sont méritants ? Nous avons posé des questions sur le budget et en fait, les choses ne sont pas très claires. Selon les informations reçues, il y aurait 2 millions de dollars, ce qui est en fait le même montant que pour la série de 2012. Ce montant se traduit en 10 à 15 candidats, donc il nous faudra réfléchir au cas où il y aurait davantage de candidats.

Lundi, nous avons parlé des différentes options et nous tirons deux décisions de notre réunion. Voilà notre travail à l'avenir. Nous avons deux options. Premièrement, attendre jusqu'à ce que nous ayons reçu toutes les candidatures, qu'elles aient été évaluées et ensuite, on pourra déterminer quel sera le niveau de soutien. Ce que cela veut dire, c'est que suivant le nombre de candidats qualifiés qui sont sélectionnés, le montant sera divisé de manière égale entre eux sauf si un candidat dit : « Non, je n'ai

pas besoin de tout le soutien. » Dans ce cas, il recevra le soutien qu'il souhaite et le restant sera divisé entre les autres candidats.

L'option 2. First-in, first out, donc premier arrivé, premier sortant. On lance les candidatures, les gens se présentent et ils sont informés de leur qualification. Mais plutôt que de leur dire combien, on leur donne en fait une plage de soutien, 50 % à 75 %. Et lorsque le processus est terminé, le montant exact qu'ils recevront leur est communiqué.

Pour les deux options, il nous faut réfléchir à la fermeture du processus. Ce processus de candidature, c'est 18 mois avant le début de la prochaine série. Nous avons parlé aux SubPro de clore avant la prochaine série, mais peut-être que des personnes seront informées un peu plus tard, peut-être deux mois avant le début de la série. Mais deux mois, c'est aussi trop proche de la prochaine série. On n'a pas encore réfléchi à tout cela.

Nous avons parlé de l'utilisation de fonds des produits des ventes aux enchères, mais nous n'avons pas encore quoi que ce soit de concret. Nous devons encore réfléchir. L'idée, c'est qu'on pourra peut-être en parler la semaine prochaine. Le personnel doit aussi réfléchir aux pours et aux contres des options 1 et 2, donc on y reviendra.

Voilà, je crois que c'est tout. Merci.

OLIVIER CRÉPIN-LEBLOND : Merci d'avoir été aussi efficace.

Nous avons une main levée de Michael Palage.

MICHAEL PALAGE : Merci.

Sarah, je vous remercie pour cette présentation. Étant donné les options qui sont limitées, je me demandais, est-ce que vous avez réfléchi à une troisième option ? J'avais écrit un document pour le [PRV] avant Cancún et j'avais parlé d'un menu à la carte. L'idée, c'était plutôt que de demander des frais d'un quart de million de dollars aux candidats, est-ce qu'on ne devrait pas plutôt diviser les frais en différentes phases ? De cette manière, cela permettrait de baisser les coûts généraux et d'être plus inclusifs.

Les deux options que vous avez, qui sont en fait vos devoirs, votre travail à venir, limitent les options de maximisation pour les participants. Je me demandais, est-ce qu'il pourrait peut-être y avoir d'autres options ou est-ce que vous êtes limité à ces deux options et que vous restez cantonnés sur cela ?

SARAH KIDEN : Merci Michael. Peut-être que vous pourriez partager le lien vers le document que vous avez écrit, ce serait très utile.

Nous avons parlé de beaucoup d'options en fait, et au sein du groupe de travail, nous nous sommes arrêtés sur ces deux-là parce qu'à chaque fois qu'on propose quelque chose, quelqu'un disait : « Ceci n'est pas possible, ce n'est pas acceptable, ce ne sera pas envisageable. » Il y a donc beaucoup de scénarios. Par exemple, la réduction des frais de candidature, nous avons parlé d'exemption de frais ; beaucoup d'options ont été débattues. Mais voilà les deux options viables que nous avons retenues. Ceci étant, nous pouvons toujours revenir vers le groupe de travail et je pourrai leur demander si votre autre option est possible.

MICHAEL PALAGE : Très bien, je vais faire ceci, Sarah. Peut-être que vous pourriez mettre votre e-mail dans le chat et je vous l'enverrai. Merci.

SARAH KIDEN : Merci.

OLIVIER CRÉPIN-LEBLOND : Merci beaucoup.

Je ne vois pas d'autres mains.

Sarah, sur la liste de diffusion, vous avez dit que vous alliez parler d'autres points. Est-ce que c'est le dernier appel auquel vous allez participer ou est-ce qu'on va vous revoir ?

SARAH KIDEN : Je suis là jusqu'à la fin du mois.

OLIVIER CRÉPIN-LEBLOND : Très bien, alors on ne vous dit pas adieu tout de suite.

SARAH KIDEN : Oui, c'est cela.

OLIVIER CRÉPIN-LEBLOND : Merci beaucoup pour cette mise à jour. Désolé que cela ait été aussi rapide.

Nous allons maintenant demander à Hadia de nous faire une mise à jour sur les commentaires des politiques.

HADIA EL MINIAWI : Merci beaucoup.

Récemment ratifié par l'ALAC, aucun.

Commentaire public ouvert, nous avons la proposition de gouvernance PTI-IANA qui sera traitée par le groupe de travail

OFB. Si cela vous intéresse, n'hésitez pas à rejoindre le groupe de travail de l'OFB et ses appels.

En cours de révision, nous avons les amendements à la charte de l'unité constitutive des fournisseurs de services Internet et des services de connectivité qui sera clos le 26 juin, également géré par le groupe de travail OFB.

Il y a aussi par le CPWG l'EPDP sur le rapport initial de phase 1 sur les noms de domaines internationalisés. L'équipe CPWG présentera la déclaration à la fin du mois, le dernier mercredi du mois. Entre-temps, nous faisons le suivi régulièrement toutes les semaines par rapport à ce rapport en faisant des présentations.

Ensuite, nous avons les amendements aux statuts et les documents pour mettre en œuvre la révision du NomCom qui est également géré par l'OFB. Judith Hellerstein et Yrjö Länsipuro sont les rédacteurs de cette question, encore une fois avec l'OFB.

Et nous avons la proposition de renouvellement du contrat des opérateurs de registre pour le .net. Michael Palage et Bill vont présenter cette question aujourd'hui. Je ne sais pas si je leur cède la parole maintenant. Michael et Bill, est-ce que vous êtes prêts ?

MICHAEL PALAGE : Oui.

HADIA EL MINIAWI : Très bien, alors allez-y.

MICHAEL PALAGE : Rapidement, Jonathan, j'étais en train de regarder mes mails, est-ce que vous voulez bien montrer la proposition ou est-ce que vous avez autre chose à proposer ? Je n'ai pas tout lu en fait.

JONATHAN ZUCK : Désolé. Michael a préparé une proposition qu'il a fait circuler dans la petite équipe. C'était hier ou peut-être que c'était la veille, je sais plus. Mais apparemment, le langage n'était pas celui que nous utilisons d'habitude. L'idée, c'était de nettoyer ceci et je ne sais pas si Michael l'a lu.

MICHAEL PALAGE : Non, je ne l'ai pas lu. Comme je vous le disais, j'étais un petit peu préoccupé par autre chose.

JONATHAN ZUCK : Effectivement, du coup, nous avons deux projets préliminaires à vous montrer. Peut-être qu'il faudrait qu'on s'en occupe au sein

de la petite équipe et qu'on le mette dans un document Google pour que les gens puissent faire leurs commentaires.

Dans un premier cas, il y a une version un peu complexe qui a besoin d'être simplifiée. Et l'autre document, c'est un document plus simple mais qui a peut-être besoin d'être revu. Voilà, il y a deux approches. J'ai essayé de le mettre un petit peu à notre sauce, pour ainsi dire. Je ne sais pas s'il faut en parler maintenant.

Vous vous rappelez peut-être que lors de notre dernière réunion, Bill et Mike ont fait une présentation sur les différents points qu'il nous semblait important de soulever. Nous avons ensuite résumé ceci en trois points et recommandations dans le cadre de ce commentaire public. Peut-être bien qu'on ira au-delà du commentaire public et qu'on passera un avis. Mais pour l'instant, c'est un commentaire public qui doit être envoyé assez rapidement et il faut que l'ALAC ait le temps de lire.

Je ne sais pas, Chantelle si peut-être vous pouvez faire apparaître les deux versions, ma version et…

MICHAEL PALAGE : Je ne crois pas que Chantelle soit là aujourd'hui.

JONATHAN ZUCK : Oui, c'est vrai. Si je suis co-hôte, je peux peut-être vous montrer la recommandation.

HADIA EL MINIAWI : Nous sommes prêts à l'afficher pour vous si vous voulez.

JONATHAN ZUCK : Vous avez ma version ?

HEIDI ULLRICH : Oui.

JONATHAN ZUCK : Je voulais veut attirer votre attention sur les recommandations sur lesquelles nous nous sommes mis d'accord. Vous les avez là en caractères gras. En conjonction avec les parties contractantes, on devrait explorer la mise en place des obligations… Attendez.

La première question, c'est celle qui a été soulevée par Evan Leibovitch au tout début. Il s'agit du texte relatif à Verisign, la possibilité qu'ils puissent éliminer des sites suite à une ordonnance juridique ou suite à une demande gouvernementale. Ce qui aurait dû ressortir de ces conversations, c'est l'idée qu'il faudrait peut-être documenter tout ceci davantage et divulguer ces ordonnances.

Ce texte n'existe dans aucun contrat, donc il faut s'assurer que les parties contractantes soient informées, quelle est la fréquence de ces ordonnances, etc. Je crois que c'est là-dessus qu'on s'est concentrés et je crois qu'on on s'est mis d'accord là-dessus au sein de la petite équipe. Michael, vous pouvez me dire si je me trompe, mais je crois que c'est quelque chose qu'on peut emprunter aux contrats de base.

MICHAEL PALAGE : Vous voulez que je vous réponde ou pas ?

JONATHAN ZUCK : Oui. Je ne veux pas parler en votre nom, j'essaie simplement de procéder rapidement.

MICHAEL PALAGE : Oui, pas de soucis.

Par rapport à ce que vous venez de dire, Jonathan, sur la base du commentaire de [Zack] et d'Evan, c'est selon nous quelque chose qui était important à ajouter puisque la majorité des commentaires publics se concentrent sur cette question.

Il y a une chose que j'ai essayé de faire dans ma discussion détaillée et c'était de me concentrer sur la lettre d'intention, parce que la lettre d'intention qui a été amendée et qui inclut le

.net et le .com parle de l'obligation de meilleures pratiques. C'est une des raisons pour lesquelles j'avais demandé à Graeme où on en était par rapport aux signalements de PIR ; pour moi, c'était un bon exemple. Voilà un petit peu pourquoi je suis rentré dans le détail dans la première version.

Bien sûr, l'approche que j'avais utilisée pour cette version préliminaire était en deux parties. Il fallait documenter quelque chose de nouveau par rapport à ce qu'on nous avait demandé de faire, d'utiliser ce genre de texte. Aussi, nous voulions avoir l'opportunité d'utiliser du nouveau texte et utiliser l'accord de base pour déterminer les différences entre le texte qui existait auparavant et un texte qui sera utile.

La prochaine recommandation ici, il s'agissait de l'ICANN qui devrait se préparer pour une comparaison détaillée du .net. Mike a fait du très bon travail dans ce sens pour utiliser différents textes pour savoir quelles sont les modifications à faire, les choses sur lesquelles on devrait se concentrer dans l'avenir pour pouvoir faire cette comparaison. Il y a des choses qui ne sont pas forcément logiques puisque les documents sont différents. Il y a des versions différentes de ces mêmes documents. L'idée était de faire des comparaisons et de se focaliser sur l'intérêt public général. Voilà la deuxième recommandation.

JONATHAN ZUCK : Michael, je lis votre document en même temps. Lorsqu'il s'agit de la ligne rouge, je pense que le Conseil d'Administration de l'ICANN a spécifiquement demandé que l'on adopte des accords de base différents en ce qu'il s'agit de l'accord des bureaux d'enregistrement pour tout ce qui est lié à l'intérêt public général.

JONATHAN ZUCK : Il faut revenir en arrière dans la conversation. L'IRT est revenu avec des recommandations différentes sur cela. Il faut résoudre cela. Je parle de recommandations différentes. On va mettre quelque chose sur la liste pour pouvoir faire des commentaires sur ce document afin de résoudre le problème.

Il y a un autre élément qui en est ressorti. Il s'agit de la notion de langage utilisé. Dans l'accord de base des opérateurs de registre, il y avait des majuscules utilisées alors qu'avant, on avait utilisé des lettres minuscules beaucoup durant plusieurs années. Ce qu'on voulait faire, c'est d'expliquer pourquoi cela s'est produit dans cet accord de base et ainsi, on pourrait faire des mises à jour sur le langage qui correspond dans cet accord du .net.

Il y a une différence significative entre les deux accords. Ce n'était pas accidentel, c'était tout à fait intentionnel et il faut

qu'on fasse un suivi et une demande pour que les mêmes changements soient adoptés dans l'accord .net avec les opérateurs de registre. Ceci implique un mandat un peu plus large de la communauté lorsqu'il s'agit de politique de consensus.

Ensuite, il y a des discussions sur les recherches économiques. L'accord de base des opérateurs de registre détermine un langage pour la participation raisonnable sur les recherches économiques de la part des opérateurs de registre. Cela n'est dans l'accord du .net. On va requérir ceci pour que cela fasse partie du plan stratégique quinquennal. L'ICANN Org a besoin d'une analyse économique compréhensive dans le marché de noms de domaine. Voilà les recommandations importantes.

Maintenant que Mike est de retour, il va nous aider à comprendre de façon plus détaillée ce document. Nous n'avons que très peu de temps pour cela car nous devons présenter cela à l'ALAC avant de rentrer dans la période de commentaires publics. Nous allons mettre cela sur la liste dans les jours à venir et nous allons donner suffisamment d'explications pour que vous puissiez bien comprendre pour qu'on puisse arriver à faire des modifications.

Quelque chose à rajouter à cela, Mike ou Bill puisque vous êtes en ligne ?

MICHAEL PALAGE : Oui, ça va, merci.

JONATHAN ZUCK : Nous avons nos devoirs à faire et vous avez aussi vos tâches à accomplir. Ainsi, vous pourrez poser vos questions et faire vos commentaires sur cette version préliminaire.

Olivier, vous reprenez la parole ?

OLIVIER CRÉPIN-LEBLOND : Oui, merci Jonathan. Nous allons vous redonner la parole, à vous et à Hadia, pour discuter de l'ICANN77.

JONATHAN ZUCK : Hadia.

HADIA EL MINIAWI : Pour planifier l'ICANN77, nous avons trois séances sur les politiques. La première séance sera liée à la perspective des utilisateurs finaux vis-à-vis de la nouvelle série de gTLD. Nous allons faire passer un lien pour cette session. Ensuite, nous avons une session interne qui sera gérée par Cheryl sur la prochaine série de priorisation. Ensuite, nous avons une séance

sur les politiques, une section pour les comités croisés sur les enchères. Ce sera géré par Jonathan.

Rapidement, je voudrais parler de cette première séance qui sera liée aux politiques.

OLIVIER CRÉPIN-LEBLOND : Nous n'avons pas beaucoup de temps.

JONATHAN ZUCK : Je pense que nous en avons parlé déjà durant notre dernier appel. Nous avons planifié d'autres appels pour cela. Si des personnes veulent participer à ces séances, les informations seront envoyées avec le document Google.

HADIA EL MINIAWI : Très bien.

Voici les éléments de discussion qui ont été établis. Vous pouvez cliquer sur le lien. Nous avons un lien aussi pour le rapport des séances. En fait, il y aura aussi des liens pour le calendrier de l'ICANN77, les séances d'At-Large, tous les points nécessaires de discussions. Il y a aussi un lien pour toutes les séances diverses et pour la séance de récapitulation.

Je vais donner la parole à Jonathan pour voir s'il a quelque chose à rajouter.

JONATHAN ZUCK : Non, je ne pense pas. Je pense que nous avons déjà dépassé le temps imparti. Les plans sont en cours, tout se déroule bien. Nous avons un peu moins d'un mois avant cette réunion de l'ICANN77 à Washington D.C. Je remercie tout le monde.

OLIVIER CRÉPIN-LEBLOND : Merci Jonathan, merci Hadia.

Nous avons terminé avec cet appel. En attendant, y a-t-il d'autres sujets de discussion ? S'il n'y a rien d'autre à discuter, nous allons en terminer avec cet appel.

YEŞIM SAĞLAM : Merci. Notre prochain appel aura lieu le 24 mai à 19 h UTC, donc mercredi prochain.

OLIVIER CRÉPIN-LEBLOND : Merci à tous. Mercredi le 24 mai à 19 h UTC.

Merci à tous d'avoir participé à cet appel aujourd'hui. Merci surtout à Graeme Bunton pour sa présentation. Merci à toutes les personnes qui nous ont fourni des mises à jour et à tous les participants, aux contributeurs et au service de transcription. D'ailleurs, je voulais dire à tout le monde, lorsque vous fermez votre page Zoom, il y a souvent un questionnaire, un petit

sondage qui pourrait être utile par la suite. Merci beaucoup à tous.

Bon après-midi, bonne journée à tous et à la prochaine fois. Hadia, je ne vous ai pas demandé par contre si vous avez quelque chose à rajouter.

HADIA EL MINIAWI : Non je n'ai rien à rajouter, merci beaucoup.

OLIVIER CRÉPIN-LEBLOND : Au revoir à tout le monde.

YEŞIM SAĞLAM : Merci de nous avoir rejoints aujourd'hui. La réunion est ajournée. Bonne fin de journée, au revoir.

[FIN DE LA TRANSCRIPTION]