ICANN83 | Forum de politiques – Séance conjointe : ALAC et SSAC
Mardi 10 juin 2025 – 09h00 à 10h15 CEST

YESIM SAGLAM

La séance va maintenant commencer. Nous allons lancer l'enregistrement. L'enregistrement a débuté.

Bonjour et bienvenue à cette séance conjointe ALAC et SSAC. Je m'appelle Yesim Saglam et je suis responsable de la participation à distance pour cette réunion.

Veuillez noter que cette séance est enregistrée et qu'elle est gouvernée par les normes de comportement de l'ICANN ainsi que les règles anti-harcèlement de l'ICANN pour sa communauté. Les questions et commentaires seront lus uniquement s'ils sont soumis dans le cadre questions-réponses, dans cette fenêtre.

Nous allons avoir l'interprétation en anglais, français et espagnol aujourd'hui. Si vous voulez prendre la parole durant cette séance, veuillez lever la main sur Zoom et une fois qu'on vous donnera la parole, vous aurez la permission d'ouvrir votre micro sur Zoom. La participation en site utilisera les micros qui sont dans la salle. Veuillez indiquer votre nom pour l'enregistrement, la langue dans laquelle vous allez vous exprimer si vous parlez une langue autre que l'anglais et veuillez parler à un rythme raisonnable.

Merci beaucoup de vous joindre à nous. Je passe maintenant la parole à Jonathan Zuck, président de l'ALAC et Ram Mohan, président de SSAC.

JONATHAN ZUCK

Oui, merci beaucoup Yesim. Nous avons une très bonne collaboration étroite avec SSAC. C'est très important de savoir ce sur quoi vous faites de la recherche actuellement et voir quelles sont vos préoccupations. Et, nous allons donc nous assurer que nos unités constitutives comprennent bien également tout ce qui se passe. Donc, merci et bienvenue!

RAM MOHAN

Oui, c'est toujours un plaisir d'être avec vous. Toujours un plaisir d'être avec l'ALAC. C'est un groupe avec qui on a toujours passé du temps où nous avons expliqué la technologie. Maintenant, c'est beaucoup plus expliquer la technologie aux autres personnes et utilisateurs parce qu'il y a beaucoup d'expertise ici et nous pouvons faire tout le jargon que nous voulons et l'utiliser, et on n'a pas besoin de vous l'expliquer. C'est vraiment un plaisir que d'être avec vous aujourd'hui.

Et, nous voyons donc cette collaboration entre l'ALAC et le SSAC comme étant absolument crucial. Et, une grande partie de cela, c'est de réaliser que SSAC fait son travail de recherche de conseils, mais la véritable valeur qui se dégage, c'est qu'une fois que c'est

fait ce travail, et bien il faut qu'il soit compréhensible dans les mains de ceux qui probablement en ont le plus besoin.

Donc, nous avons une évolution. On se satisfait du travail de recherche que nous faisons, mais là, en fait, c'est là, une fois qu'on avait…

JONATHAN ZUCK

Donc, c'est un mécanisme qui doit se poursuivre. Et dans notre communauté, nous avons une communauté At-Large qui est vraiment très importante de par sa taille. Nous avons des structures At-Large des ALS et nous avons toutes une couverture dans le monde et nous avons une communauté ICANN qui est importante. Donc, on va faire beaucoup d'expérience à ce niveau et nous allons effectuer des partenariats avec vous pour développer ces expériences.

RAM MOHAN

Oui, c'est excellent. C'est un autre système, en effet, qui dépasse l'ALAC et qui est très important parce que c'est ce qui fait avancer les choses. Et donc, Jonathan, il faut que les documents et les matériaux soient plus accessibles.

Donc, ce que nous effectuons, c'est que pour beaucoup des documents SSAC nous avons nos membres qui font des résumés de 500 mots qui capturent l'essence même du document et on essaye de travailler avec vous étroitement pour que littéralement on

trouve des manières, que cela soit présentable et accessible aux utilisateurs.

JONATHAN ZUCK Oui, c'est une danse en fait que nous effectuons.

RAM MOHAN Donc, SSAC je crois, il y a quelques semaines, a publié un document qui s'appelle le SSAC127. C'est sur le blocage du DNS et les nouveautés à ce niveau. Et, il va y avoir une présentation aujourd'hui à ce sujet. En ce qui concerne les recherches, les résultats clés qui ont été développés à partir de ce travail. Et, donc, nous nous engageons avec vous. Nous travaillons avec le GAC également. Comme vous le savez, nous savons que les gouvernements sont très intéressés par cela. Ils utilisent très souvent le blocage du DNS. C'est un réflexe qu'ils ont parfois pour diverses raisons, et nous sommes ici pour éclairer un petit peu ce qu'est le blocage du DNS et également indiquer à quel point cela peut être parfois problématique. Donc, nous allons passer à la diapo suivante.

WARREN KUMARI Donc, qui va passer la présentation? Bien. Est-ce que l'on peut passer à la diapo suivante s'il vous plaît? Je vais soulever mon chapeau. Voilà, donc, c'est très joli. La prochaine diapo est très très belle. Il y a une très très belle photo de Prague sur cette diapo. On

a beaucoup de diapos donc j'aimerais qu'on puisse passer ces diapos.

Donc je peux parler, je peux parler.

Donc à la base, en 2011 2012, et bien SSAC a publié un SAC50/SAC56. L'Internet a depuis beaucoup changé en douze treize ans, une forte évolution et on a décidé qu'il fallait mettre à jour le document et fournir de nouveaux avis et opinions au sujet du blocage du DNS. Et, donc, voilà! Voilà, c'était une très belle photo qu'on a vue et maintenant nous avons donc la diapo suivante, on peut avancer dans la présentation. Oui, voilà, très bien.

Donc, l'objectif du document, c'est pour les décideurs et pour les responsables gouvernementaux de parler des implications, des conséquences et des dangers d'utilisation du blocage du DNS. Qu'est-ce qui peut poser problème à ce niveau? Diapo suivante s'il vous plaît! Alors, qu'est-ce que c'est que le blocage du DNS? Et, bien, le blocage du DNS, c'est une technique pour bloquer l'accès aux contenus sur l'Internet, donc c'est un filtre qui utilise les résolveur du DNS. Ça, c'est pour que plusieurs utilisateurs, un groupe d'utilisateurs, ne puissent pas atteindre leur contenu. Cela impacte les utilisateurs qui utilisent donc certains résolveurs lorsqu'il y a donc ces résolveurs qui bloquent l'accès aux DNS.

Et, ce que cela accomplit. Nous allons voir cela à la diapo suivante. Et, bien, c'est cela. Ça ne passe pas. Et, si vous utilisez un résolveur récursif et qu'il y a un blocage du DNS, et bien vous n'allez pas être

en mesure d'accéder au contenu qui est bloqué. Mais, comme cela a été noté auparavant, cela n'est pas totalement efficace et cela ne s'applique qu'à certains. Donc, diapo suivante s'il vous plaît.

Donc, le blocage DNS, c'est simplement un outil et comme tout outil, il peut être utilisé pour différents objectifs à des forces et des faiblesses. Et, il faut comprendre comment fonctionne cet outil parce que sinon vous allez ne pas bien l'utiliser et vous pouvez vous blesser. Donc, c'est un outil puissant quand même, comme tous les outils puissants, et bien si vous ne savez pas l'utiliser, les conséquences vont être néfastes.

Et, il n'y a pas de retrait du contenu ou de service de l'Internet. C'est simplement inaccessible à un ensemble d'utilisateurs. Donc, c'est plus limité si vous voulez. Ce n'est pas une suspension de nom de domaine par exemple. Et, c'est plus approprié. C'est parfois la seule option qui est disponible à une pour une communauté, pour un ensemble d'utilisateurs. Donc, comme je l'ai mentionné plusieurs fois, ce n'est pas non plus efficace à 100 % et on peut tourner autour. Si vous voulez du blocage du DNS, et nous allons voir cela d'ici peu. Diapo suivante, s'il vous plaît.

Voilà. Alors, comment est-ce que l'on procède pour faire le blocage du DNS? Ici, vous avez un aperçu de la résolution DNS et avec le blocage du DNS sur le serveur récursif de DNS, c'est celui du milieu, il y a un filtre qui s'applique. Lorsqu'un utilisateur fait une requête DNS, la requête passe par le serveur récursif et si le domaine n'est pas sur la liste de blocage, alors la résolution DNS a lieu

normalement et l'utilisateur peut avoir accès au contenu. En revanche, si le nom de domaine figure sur la liste de blocage, plutôt que d'avoir accès à l'information, il y a autre chose qui se passe avec cette requête DNS et normalement l'utilisateur n'a pas accès au contenu.

Donc, lorsque je dis que quelque chose d'autre se passe, sachez qu'il y a plusieurs choses qui peuvent se produire. D'abord, la chose la plus courante et potentiellement moins dommageable pour l'utilisateur, c'est la chose suivante, Le serveur récursif répond ce nom de domaine n'existe pas. Donc, quelqu'un essaie d'avoir accès à foo.bar.com et il n'y a pas accès.

Alors, le serveur récursif envoie la réponse suivante, ce nom de domaine n'existe pas, l'utilisateur n'a donc pas accès à ce nom de domaine. Diapo suivante s'il vous plaît. Autre cas de figure, le résolveur récursif peut modifier la réponse du serveur faisant autorité et donner en retour une adresse IP autre que celle du domaine bloqué. C'est ce qu'on appelle redirection et c'est quelque chose que l'on voit appliquer assez souvent. Donc c'est l'une des options considérées comme les moins bonnes en raison de résultats assez mauvais au niveau de la sécurité.

Troisième option qui pour plusieurs semble la meilleure, c'est que le résolveur récursif peut parfois ignorer la requête. Si l'utilisateur demande un domaine en particulier, le résolveur récursif peut tout simplement ignorer cette requête et ne pas y répondre du tout. Mais, l'inconvénient de cela, c'est que la plupart des utilisateurs

ont plusieurs résolveur récursif sur leur liste et si le premier ne répond pas, alors ils demanderont au deuxième, troisième ou quatrième résolveur récursif si ce résolveur récursif applique ce blocage, alors l'utilisateur peut modifier le nom et avoir accès au contenu qui est supposé être bloqué. Et, comme je vous l'indique en bas de cette diapo en italique, et cela n'affecte réellement que le résolveur récursif ou le blocage a lieu. C'est à dire que si l'utilisateur utilise un autre résolveur récursif, alors il peut contourner ce blocage DNS.

Donc, le blocage DNS, c'est en quelque sorte une saisie ou suspension de domaine, mais d'une autre manière. C'est à dire que les gens peuvent utiliser plusieurs résolveur récursif tandis que la saisie de domaine c'est retirer le nom de domaine totalement de l'internet, donc c'est différent. Cette suspension ou saisie de domaine…

OK, l'enregistrement a commencé. Bonne nouvelle. Oui, c'est ça la nouvelle technologie. Et, j'ai un écho maintenant quand je parle, je ne sais pas qui a activé son micro, mis à part le mien. Donc, la saisie de domaine finit par passer par le serveur faisant autorité au bureau d'enregistrement opérateur de registre. Donc, la saisie de domaine est en général utilisée pour la suppression des réseaux zombies ou des sites d'hameçonnage ou d'infraction aux droits de propriété intellectuelle. Donc, ça touche les serveurs faisant autorité, bureau d'enregistrement ou opérateur de registre, ça affecte tout le monde.

Et cet outil est un peu plus large puisque ça affecte tous ceux qui utilisent un nom de domaine. Mais parfois, c'est la seule option disponible. Par exemple, en cas d'infraction de droits de propriété intellectuelle, vous pouvez avoir une saisie ou une suspension de domaine alors que vous ne pourriez pas aller trouver tous les résolveur récursif pour leur demander la même chose. Donc, je regarde ma montre, il faut que j'accélère je crois.

JONATHAN ZUCK Nous n'entendons pas. Donc, la question est qu'est-ce que fait cette grande image qu'on voit ici à l'écran?

WARREN KUMARI Je vois qu'on est enregistré deux fois ici. Donc, ici, on regarde les requêtes qui ont lieu ici et répond à différentes réponses. Donc, on ne fait pas ce qu'on appelle un blocage de DNS. C'est plutôt une attaque de l'homme du milieu ou quelque chose de ce type.

Donc, motivation. Exemple, pourquoi est-ce que les gens font cela? Il y a toute une série de motifs. Peut-être que la moins controversée, c'est les opérateurs de réseaux qui font du blocage DNS sur leur résolveur récursif. Excusez-moi, j'étais en train de modifier les diapos sur mon ordinateur. Voilà, celle-ci… Donc, un nombre significatif de résolveur récursif font d'ores et déjà cela. Si on sait qu'il y a sur ce site des logiciels malveillants ou bien s'il y a des réseaux zombies beaucoup de résolveur récursif vont opérer ce type de blocage. L'un des plus connus, c'est CloudFlare qui

fonctionne sur 1.1.1 avec une deuxième adresse 1.1.2. Ils peuvent décider de configurer ça sur leur machine et ça, ça va bloquer une série de noms de domaine.

Diapo suivante. Là, un exemple un peu plus controversé, c'est à dire que beaucoup d'entreprises ont des politiques de leur société qui stipulent que les entreprises, les employés ne devraient pas aller sur tel ou tel site pendant leurs heures de bureau. Et, donc, ils peuvent mettre en place un blocage en souscrivant à la liste de blocage et l'appliquer à leur résolveur récursif et si un utilisateur essaie d'avoir accès à Facebook par exemple, alors le résolveur récursif peut bloquer cela et les renvoyer autre part.

Autre exemple, certaines organisations telles que les écoles, les bibliothèques, etc. appliquent un blocage d'accès pour tout contenu inapproprié, c'est à dire accès à des sites de jeux ou de pornographie, etc. Donc, comme je vous l'ai dit auparavant, CloudFlare à 1.1.1 et également 1.1.3 qui bloque l'accès aux logiciels malveillants et bloque le contenu, donc si vous êtes parent et vous voulez éviter que vos enfants aient accès à un contenu inapproprié, vous pouvez utiliser ce 1.1.3 comme exemple pour bloquer ce type de contenu.

Ça, c'est un exemple beaucoup plus connu et d'une certaine manière plus controversé. Il peut s'agir de blocages mandatés par le gouvernement ou par un tribunal, ou le gouvernement ou un tribunal mandate le blocage d'accès à un certain nombre de domaines. C'est ce qu'on appelle un mécanisme de censure, c'est

à dire le contenu offensif ou susceptible de déstabiliser le gouvernement. Le gouvernement peut demander aux opérateurs FSI de leur pays de bloquer l'accès à un domaine particulier. Il y a une série d'études de cas dans ce document. Là, c'est un bref aperçu, mais je vous invite à lire ce document et je suis sûr que vous serez nombreux à ne pas le faire. Mais, s'il vous plaît, faites-le. Lisez ce document.

Le SSAC essaie de s'en tenir aux éléments techniques dans ce document et nous ne prenons aucune position par rapport à la censure ou à des cas particuliers, mais nous vous invitons de nouveau à lire ce document pour avoir de plus amples détails. Diapo suivante. Donc, comme je l'ai dit à plusieurs reprises, le blocage de DNS n'est que partiellement efficace. En bas de cette diapo, on voit une résolution normale du DNS. L'utilisateur envoie sa requête à son résolveur récursif. Si le nom n'est pas sur la liste de blocage, alors il a accès au domaine. S'il y figure sur la liste, alors la DNS. La résolution DNS ne fonctionne pas ou il est redirectionné.

JONATHAN ZUCK Alors, une question par rapport à ce graphique. En bas dans l'exemple, vous avez une flèche, mais rien n'indique ce qui se passe lorsqu'on passe le filtre au niveau du résolveur récursif?

WARREN KUMARI Oui, alors ça n'est pas nécessairement un graphique brillant, c'est simplement pour montrer que si le nom ne figure pas sur la liste de

blocage, alors il n'est pas bloqué. S'il y figure, il est bloqué. C'est simplement pour montrer où ça va. Je ne sais pas si j'ai répondu à votre question, mais oui, ce graphique, effectivement, peut porter à confusion. Ça, c'est censé être le résultat de la décision et non pas où se trouve la demande de l'utilisateur. Donc, tout cela s'applique uniquement si la requête de l'utilisateur passe par le résolveur FSI. Mais, s'il passe par un autre résolveur où il n'y a pas de blocage, alors le blocage ne va pas être efficace. Diapo suivante s'il vous plaît!

Alors, comment tout cela fonctionne? L'utilisateur peut utiliser un résolveur alternatif et non pas celui qui est fourni par son FSI ou par son pays. Il y a une série de manières de procéder. La plus connue, ce sont les résolveur récursif public. Il y en a un certain nombre. Google Public DNS, Cloudflare en a un, Quad9 aussi et il y a des résolveurs sponsorisés par le gouvernement comme le DNS4EU.

Et, il y a une image assez connue du printemps arabe avec un blocage DNS dans certains pays. L'image bien connue était celle de l'Egypte avec des gens qui taguaient des choses sur les bâtiments. Donc, si vous voulez accéder à un contenu… À un contenu qui avait été bloqué, vous pouvez y avoir accès par l'intermédiaire de ce résolveur. Donc, c'est assez facile à utiliser et on a vu que 21 % des utilisateurs utilisent actuellement certains de ces résolveur public bien connu. Diapo suivante s'il vous plaît.

Si vous avez regardé du contenu en streaming, vous aurez vu qu'il y a beaucoup de pubs pour les VPN. L'objectif, c'est de renforcer la

confidentialité et l'anonymisation pour les utilisateurs. Mais, ce que disent également ces entreprises, c'est permettre une restriction géographique. C'est à dire que si vous voyagez et vous voulez voir un contenu qui n'est disponible que dans votre pays, vous pouvez installer un VPN et y avoir accès. Et, donc les contenus géo-restreint vous seront disponibles comme si vous étiez dans votre pays.

Autre cas commun, si vous êtes dans votre pays d'origine et vous voulez regarder un contenu qui n'est pas disponible dans votre pays. Vous pouvez installer un VPN et choisir un autre pays pour avoir accès à ce contenu comme si vous n'y étiez pas. Donc, ce que cela veut dire, c'est que lorsqu'il y a un blocage de DNS ou du filtrage DNS dans votre emplacement, vous pouvez utiliser un VPN et donc tourner autour de cela.

Et, c'est très simple, c'est de plus en plus simple à effectuer et utiliser ces VPN. Vous avez des services de streaming qui offrent cela pour regarder en ligne et vous pouvez donc avoir divers types d'équipements comme des téléphones. Donc, par exemple, il y a des relais Apple que vous pouvez allumer et vous pouvez donc utiliser ces VPN comme CloudFlare également, qui offre des VPN, des services VPN pour donc le respect de votre vie privée et donc un DNS alternatif. Nous allons passer à la diapo suivante.

C'est assez similaire par rapport à ces réseaux privés virtuels. C'est en rapport avec Tor. Sait fournit aux dissidents, aux journalistes qui réussissent à sortir des informations de leur pays. Donc, il y a des

protections de ces données avec différents nodes. Donc, ceux-là, c'est un chiffrement si vous voulez du trafic internet dans différents nodes. Ça marche très bien, mais cela permet donc de ne pas passer par les filtres du DNS et donc de faire sortir de votre pays des données. Nous allons passer à la diapo suivante.

Il y a également la validation DNSSEC. Ça c'est conçu pour détecter et atténuer donc les personnes qui essayent d'effectuer des usurpations. C'est comme cela que cela fonctionne. Cela change la réponse de DNS du serveur qui fait autorité. Et, ce que l'on voit de plus en plus, c'est que les services d'opérations, donc ont des résolveurs qui sont validés au niveau local.

Et, donc la distribution a un résolveur de validation et vous avez les routeurs que vous achetez ont des validations de DNS et s'il y a un blocage qui se fait à ce niveau, et bien au niveau du résolveur privé, ça va être détecté et détecté qu'il y ait un problème et le résultat ne va pas être le bon et on va passer au résolveur suivant dans la chaîne. S'il n'y a pas le filtrage du DNS à ce niveau, et bien le filtrage ne va pas s'effectuer.

Donc, je devrais peut-être avancer un petit peu plus vite. Et, ce qu'il faut retenir de cela en tout cas, c'est que le succès ou l'efficacité du blocage du DNS, c'est souvent par degré. Ce n'est pas complet, ce n'est pas quelque chose qui fonctionne totalement, mais ça permet donc pour des utilisateurs qui utilisent un ensemble de résolveurs vont avoir un blocage, mais les utilisateurs peuvent contourner

relativement facilement ce blocage du DNS comme on l'a vu. Nous allons passer à la diapo suivante.

Et, la diapo suivante. Donc, le DNS, ça, ce sont des technologies depuis de nombreuses années qui sont utilisées. On a parlé beaucoup du HTTPS pour avoir plus de sécurité. On a amélioré les protocoles, mais le DNS…il y a toujours des fuites au niveau DNS si vous voulez. Et, pour limiter cela, et bien l'IETF et les groupes d'ingénierie informatique, et bien ont essayé de protéger le DNS avec plusieurs méthodes, avec des chiffrement, des requêtes et des réponses. Donc, il y a plusieurs niveaux, plusieurs couches. Il y a le TLS, le Dox, le DNS sur QUIC, différents types de transport.

Donc, ça c'est les réponses qui sont chiffrées, les requêtes qui sont chiffrées et qui sont comme toutes autres données. Donc, cela veut dire que les utilisateurs peuvent mettre à jour leur système de résolution pour utiliser donc un résolveur chiffré ailleurs. Et, ça, ça ne va pas être détectable. Ça va être donc un système de filtrage. Il ne va pas pouvoir y avoir de blocage et le blocage va être contourné. Ça ne va pas être visible au niveau du réseau lorsqu'on utilise ces techniques de chiffrement.

Également, nous avons des erreurs de DNS étendues. Vous savez, lorsque vous avez ces codes d'erreur 14. Et, ça, ça a trait également au blocage du DNS d'une manière traditionnelle. Le DNS a fourni que très peu d'informations aux utilisateurs lorsqu'il y a des résolutions qui ne fonctionnent pas. Vous avez un message d'erreur, vous avez server failed que le serveur n'a pas fonctionné.

Vous avez ce type de message qui apparaît à l'écran. Mais, avec ce nouveau RFC, et bien on peut annoter les messages d'erreur du DNS. Il y a différents codes qui peuvent être appliqués.

Par exemple le code 16, donc erreurs DNS étendues censurées. Donc, cela indiquerait que le nom de domaine n'existe pas. Donc, par exemple, si une cour de justice ou une partie externe a limité cela, a limité l'accès à ce nom de domaine. Donc, peut-être que c'est sur une liste de blocage. Peut-être que vous avez utilisé un filtre pour bloquer avec par exemple les contenus réservés aux adultes. Passons à la diapo suivante et on avance encore dans la présentation.

Alors, ça, c'est un outil qui a des implications fortes. Vous pouvez avoir des conséquences inattendues lorsque l'on fait du blocage du DNS. Par exemple, si par accident vous pouvait bloquer, tous .com cela poserait un grave problème. Voyons la diapo suivante.

Il y a donc des dommages collatéraux si on n'utilise pas la bonne infrastructure. Donc, si par exemple vous essayez de bloquer le nom de serveur Akamai, et bien là vous allez avoir un nombre important de personnes qui vont être impactés. Donc, vous voyez l'étude, le document que nous avons publié, qui a beaucoup plus de détails.

Parce que, lorsque l'on parle des différents types de réponses, de blocage, et bien là, vous avez donc des messages d'erreur. Ce nom n'existe pas, ne répond pas. Pas de réponse. Il y a différents messages d'erreur qui arrivent. Donc, les résolveurs parfois

répondent de cette manière. Et, ça, ça peut être l'option la plus dangereuse. Si quelqu'un essaye d'aller à ce site, et bien il peut y avoir une redirection qui soit effectuée et on ne sait pas pourquoi il y a eu un blocage.

Le danger de cela, c'est que par définition, là où le domaine est redirigé, donc il y a des certificats TLS. Donc, lorsque l'utilisateur est envoyé là, et bien l'utilisateur va dire on essaye de voler votre information, est-ce que vous voulez continuer? Donc, là, si l'on clique sur ces aspects de sécurité importants, et bien on indique Bien, nous nous indiquons bien aux utilisateurs. Utilisez simplement HTTPS, parce que sinon vous allez avoir des problèmes au niveau des requêtes et au niveau des réponses que vous allez obtenir et aux avertissements que vous allez obtenir sur votre écran.

Donc, je crois que je ne vais pas tout présenter et passer directement aux recommandations de SSAC. Donc, trois recommandations de SSAC. La première, c'est que nous recommandons que toutes les entités comprennent bien les implications de la technologie, les forces et les faiblesses des outils et la manière d'une manière de travailler sans dommages collatéraux.

Deuxième recommandation de SSAC. Là, il y a plusieurs points. Donc, avant de faire du blocage DNS, il faut bien comprendre les implications. Est-ce que ça va être efficace? Il faut avoir une politique sur quoi bloquer et quand bloquer et revoir toute cette

décision fréquemment. Et, si vous avez le blocage du DNS, si vous l'effectuez, et bien vous devez minimiser les dommages collatéraux, donc bloquer uniquement ce qui est spécifique, le contenu que vous voulez retirer, qu'il ne soit plus visible. Et, si vous faites blocage du DNS, faites-le uniquement pour les utilisateurs dans votre juridiction.

Et, je crois qu'on est presque à la fin de ma présentation. Donc, si vous êtes des opérateurs de serveurs récursifs et que vous avez ces codes d'erreur, et bien utilisez donc 6.6 les erreurs DNS étendues pour permettre aux utilisateurs finaux de bien comprendre ce qui se passe, pour ne pas prêter à confusion, pour qu'il n'y ait pas des problèmes sur les ordinateurs, pour qu'il puisse y avoir une bonne confiance des utilisateurs finaux lorsqu'ils reçoivent ce type de message de blocage du DNS.

Très bien. Donc, je crois qu'il y a un code QR quelque part. Il ne me reste que deux trois minutes. Donc, est-ce qu'il y a des questions?

JONATHAN ZUCK

Donc, le travail commence maintenant, c'est diffuser ces informations. Qui est votre public ciblé? Qui est-ce que vous ciblez avec cela? Est-ce que ce sont les personnes qui gèrent les serveurs? Est-ce que ça ferait sens pour nous de nous concentrer sur l'application par rapport aux utilisateurs finaux? Je suis un petit peu curieux. Qui ciblait?

WARREN KUMARI

Donc, oui, qui est le nous? Donc, je crois que pour l'ALAC. Votre public, c'est peut-être des entreprises qui demandent un blocage du DNS. Si vous êtes une entreprise, une société et vous voulez faire de blocage du DNS pour que vos employés n'aillent pas sur Facebook. Voilà, ce qu'il faut garder à l'esprit. Assurez-vous qu'ils utilisent bien le résolveur de l'entreprise. Si vous faites un blocage de Facebook, et bien ne les redirigez pas quelque part parce qu'il ne faut pas ignorer le TLS.

Et, pour le public de SSAC, et bien nous c'est pour les régulateurs de gouvernements, pour les décideurs développant des politiques, pour les noms de marque par exemple le contenu pour adultes qui doit être interdit par les régulateurs, donc c'est un public très différent. Je crois que pour l'ALAC, c'est les utilisateurs qui doivent bien comprendre que si ça ne fonctionne pas, ils peuvent comprendre pourquoi ils ne réussissent pas à atteindre un site. Il faut aussi voir avec les ISP qui font du blocage. Il faut annoter, si vous voulez les blocages du DNS et si vous êtes une société qui fait cela d'une manière volontaire. Il faut garder à l'esprit tous ces points que j'ai indiqués.

RAM MOHAN

Oui, je crois qu'on pourrait revenir en effet à cette diapo où l'on parle des utilisateurs finaux et comment ils peuvent contourner donc ces questions. Je crois qu'il y a un point intéressant, là.

WARREN KUMARI

Oui, je crois que c'est la numéro 28 que l'on va… la voilà, c'est 28. La suivante. Voilà, voilà. Donc, oui, si vous redirigez les utilisateurs quelque part, foo.bar.com par exemple, et bien il va avoir une adresse IP différente qui n'est pas affilié avec bar.com, Et bien, le serveur web, donc, va être en mesure d'avoir un certificat TLS pour ce site, et le TLS est conçu pour éviter ce type d'attaques. Donc, l'utilisateur va avoir une fenêtre qui va s'afficher et ils vont voir une question pourquoi je ne peux pas arriver à ce site web?

RAM MOHAN

Oui, je me réfère à cela. Et, également est-ce que c'est une expérience normale qu'au niveau du wifi dans les aéroports, lorsqu'on utilise le wifi et que c'est très ouvert, très libre et qu'il y a pas un haut niveau de blocage? Est-ce que parfois on n'obtient pas en effet des messages de ce type qui arrivent sur les machines?

WARREN KUMARI

Oui, les portails captifs dans un hôtel par exemple. Dans un café, lorsqu'on se joint sur un réseau wifi, et bien il y a des termes de service, par exemple des politiques. Il faut cliquer. J'accepte ces termes de service et en général, lorsque vous vous connectez en premier, ils ont leur propre résolveur récursif et ils vont tout intercepter et ils vont tout contrôler et vous dire voilà, on utilise Starbucks et cliquez ici.

Et, il y avait un problème plus large. Maintenant, c'est limité un petit peu de ces jours. C'est pas totalement efficace, mais en

général, lorsque mon téléphone arrive sur un nouveau réseau Wifi, et bien le réseau peut envoyer un portail captif. Une réponse de portail captif. Vous êtes maintenant sur tel serveur ou bien l'appareil va se connecter et va avoir un navigateur qui va vous indiquer où vous êtes. Maintenant, ça se passe moins, mais cela arrive encore. Et, ce que fait ce portail captif à ce moment-là c'est en gros un blocage DNS ou un redirection d'une attaque DNS dans la plupart des cas. Est-ce que j'ai répondu à votre question?

RAM MOHAN Oui, effectivement. Oui, John?

JOHN LEVINE Oui, c'est une question assez longue, mais je vais essayer d'y répondre assez rapidement. Aux États-Unis, on a toujours eu des recommandations DNS et cette révision est très différente des autres. Avant, on disait il faut reconfigurer les noms, mais la nouvelle recommandation défend le fait que l'entreprise devrait utiliser le DNS pour protéger les réseaux qui sont mauvais pour les utilisateurs. Et très honnêtement, ils n'ont pas tort.

Mais, je pense que pourquoi est-ce qu'ils disent quelque chose de différent de ce qu'on dit? Parce qu'ils dépendent de manière critique d'un réseau. Si vous vous occupez d'un réseau pour votre entreprise, alors vous offrez un service à vos employés et si tout d'un coup les employés veut aller s'acheter quelque chose sur

internet ou quoi, il doit utiliser son portable et une connexion privée pour le faire.

Donc, si le gouvernement va bloquer tout dans un pays, alors il faut être très conservateur. Si vous êtes une organisation, le blocage doit répondre aux objectifs de l'organisation. Et, il y a le 991010 qui bloque des choses qui ne sont pas conviviales pour les familles par exemple. Voilà, le genre de choses qu'il faut prendre en considération. Donc, oui, il faut trouver un équilibre entre le blocage excessif parce qu'il y a beaucoup de bonnes choses auxquelles les gens devraient avoir accès, mais d'un autre côté, dire qu'on ne devrait pas bloquer du tout ce n'est pas une bonne chose.

WARREN KUMARI Oui, que l'utilisateur ait choisi le blocage ou pas, c'est ça la question. Si vous travaillez pour une entreprise par exemple, et que l'entreprise a une série de restrictions par rapport à ce que vous pouvez faire, alors vous êtes tenu de vous conformer à ces restrictions et pour l'entreprise, les dispositifs sont gérés de cette manière. Donc, si vous utilisez un ordinateur de l'entreprise, l'entreprise vous a obligé à utiliser une série de résolveurs et vous ne pouvez pas les changer.

INTERPRÈTE Nouvelle intervention sans micro. L'interprète n'a pas entendu.

LUTZ DONNERHACKE

Tout d'abord, merci de ce rapport. Merci parce que ça permet de retenir l'attention des gouvernements par rapport au DNS et pas uniquement avoir recours à des méthodes de blocage pour ne pas porter atteinte à l'accès des utilisateurs comme ils le pourraient. Donc, vous avez montré quelle est la manière la moins intrusive de procéder à un blocage. Et, ça, c'est bien. La plupart des résolveur récursif fonctionnent de la manière dont vous l'avez expliqué. Donc, merci de ne pas avoir expliqué comment faire un réel blocage et j'espère que ça ne va jamais être le cas. Merci.

ROBERT GUERRA

Oui, je voulais répondre à la question de Jonathan et faire un petit rappel historique par rapport au premier blocage. Je pense qu'en fait, il y a deux choses. D'abord les décideurs politiques et on voit de plus en plus, que ce soit aux Etats-Unis et ailleurs aussi, le type de contenu qui est susceptible d'être bloqué ou retiré de l'Internet qui ne cesse de croître. Et, ça, ça se fait de manière non transparente, donc si ça peut se faire par l'intermédiaire du blocage du DNS, d'après moi et d'après le SSAC, ça devrait se faire de manière aussi transparente que possible, à savoir si on va faire ça, on doit en connaître les conséquences.

Et, étant donné les développements par rapport à l'utilisation de l'Internet, voilà les conséquences si vous bloquez. Et je pense que pour les utilisateurs par rapport au portail captif et autre, si vous voulez contourner cela ou vous voulez savoir comment fonctionne

le blocage, alors c'est une question éducative et ce qu'il faut reconnaître ici.

Surtout dans certains pays du monde, il y a beaucoup de contenu qui disparaît et donc il est très important que les utilisateurs sachent comment y avoir accès. Donc, c'est un travail d'éducation et il faut que ce soit écrit de manière simple et pas simplement à l'attention de la communauté technique, parce qu'il faut bien comprendre les conséquences collatérales. Et si vous allez bloquer, il faut en connaître les conséquences et il faut permettre un flux libre d'informations en même temps.

RAM MOHAN Dernier intervenant là-dessus.

MATTHIAS HUDOBNIK Warren, est-ce que vous pourriez nous expliquer brièvement, du point de vue des utilisateurs finaux, ce qu'ils peuvent faire et ne pas faire? Je sais que ça dépend des techniques de blocage, mais en général on n'a pas un public technique ici. Donc, en deux trois phrases, quelle serait votre recommandation ou d'après vous, quelle est la chose la plus importante à retenir?

WARREN KUMARI Alors, la première chose, c'est de décider si vous voulez établir un certain type de blocage ou pas. Si vous avez décidé que vous voulez bloquer les logiciels malveillants par exemple, alors vous pouvez le faire, mais si vous êtes un utilisateur sujet au blocage que vous

voulez contourner ou éviter, alors ce que vous pouvez faire, c'est mettre à jour votre résolveur récursif, passer un résolveur public ou en fonction de là où vous vous trouvez, vous pouvez vous inscrire à un service VPN par exemple. Mais tout ça, ça dépend de la législation nationale et de votre volonté de le faire.

Par rapport au VPN, le trafic passe ailleurs et tout le trafic par le VPN. Donc, il faut que vous choisissiez un VPN de confiance. Mais, il est fort probable également que le trafic sera plus lent. Donc il faut changer votre résolveur et le faire passer par VPN.

INTERPRETE — Intervention sans micro. L'interprète n'entend pas.

RAM MOHAN — Merci. Passons à la prochaine mise à jour pour vous. Maarten est là. Il est président du groupe de travail FOSS, donc logiciel libre et à code ouvert à code source. Pardon?

MAARTEN AERTSEN — Oui, alors au SSAC nous travaillons sur un document qui n'est pas encore fini, qui porte sur l'utilisation d'un logiciel FOSS, les logiciels libre et à code source. Donc, pourquoi avons-nous fait cela? C'est parce que certains d'entre nous ont remarqué que dans les processus de développement de réglementation pour les logiciels ou les infrastructures, l'utilisation de FOSS était très réduite. Et, on

savait que si c'était plus utilisé et que s'il y avait plus de références on pourrait avancer.

Donc, dans ce document, on essaie de documenter l'utilisation de Foss dans le DNS et les caractéristiques qui les accompagnent. L'idée, c'est de faire en sorte que ce soit quelque chose de plus visible et que ce soit une ressource pour les décideurs politiques pour prendre des décisions éclairées et bien comprendre de quoi il s'agit. Donc, pour ceux d'entre vous qui ne connaissent pas bien les logiciels libres et à code source, ce sont des logiciels qui permettent à quiconque d'utiliser le logiciel, mais également d'étudier, modifier et le distribuer. Ce qui finalement s'aligne avec les idées d'origine de l'Internet par rapport à l'utilisation des logiciels.

Donc, nous sommes en train de faire des recherches dans quatre domaines. D'abord, les activités. Deux d'entre elles portent sur des activités de sondages, sondage d'enquête et deux autres sur des considérations plus politiques. Donc, d'abord deux ensembles d'infrastructures. La première infrastructure qui se concentre sur les noms de registre. Les noms de domaine des registres. On a regardé surtout ce qui se passe du côté des opérateurs registre et de l'autre du côté du DNS, c'est à dire les serveurs de noms et les résolveur DNS. Voilà, pour ce qui concerne le paysage de l'infrastructure.

La deuxième partie de ce travail porte sur une enquête par rapport aux caractéristiques des logiciels libres et à code source. En quoi

c'est différent des biens physiques et des logiciels sous propriété? Donc, on a comparé ces logiciels généraux aux FOSS qui sont très populaires dans le DNS. Troisième domaine établir une liste d'hypothèses assez communes et essayer de préciser les confusions s'il y en a. Et quatrième domaine, c'est un document d'évaluation de facteurs de risque qui nous semble important pour le développement de ce logiciel, le fonctionnement de ce logiciel et au niveau réglementaire également.

Donc, je ne suis pas venu pour vous donner des réponses ici. C'est simplement pour vous donner une idée de ce sur quoi nous travaillons. Mais, l'idée c'est de vous faire une présentation complète à Muscat et d'y inclure des lignes directrices. Donc pour la suite, nous pensons que l'utilisation continue de FOSS présente des avantages, mais également des risques. Donc, on vous soumettra plusieurs points pour considération. Voilà, je crois que je vais m'en tenir là aujourd'hui. Si on a plus de temps, je peux vous donner plus de détails. Mais, là, je me tourne vers le président pour voir.

RAM MOHAN

Alors, voyons s'il y a des questions et on va finir toutes les présentations et si on a le temps, on reviendra sur cette présentation.

EUNICE ALEJANDRA PÉREZ COELLO

Bonjour, je m'appelle Eunice et je vais parler en espagnol. J'ai une question par rapport à ce logiciel. Est-ce qu'il fonctionne avec tout système opérationnel ou pas? C'est ça la question. Est-ce qu'il fonctionne avec tout type de système opérationnel?

MAARTEN AERTSEN

Merci et excusez-moi, je n'ai pas trouvé les écouteurs pour écouter l'interprétation. Donc, par rapport à votre question, la plupart des logiciels sont disponibles pour différents systèmes. Les opérateurs en général utilisent un certain type de systèmes opérationnels et je ne peux pas dire que oui, c'est disponible pour tous, tous les systèmes opérationnels. Mais en général, pour la plupart des systèmes opérationnels, c'est le cas. Dans le rapport, on parle des applications qui fournissent les services DNS. Donc, on travaille sur cette couche, mais on sait qu'en dessous, il y a beaucoup de choses qui se passent également, mais on n'en parle pas dans le document.

RAM MOHAN

D'autres questions? Pas encore. Très bien. Donc, nous allons continuer avec nos représentations. On verra s'il y a d'autres questions. Donc, nous allons passer à la diapo suivante. C'est véritablement la prochaine présentation.

Oui. Alors, SSAC donc à lancer donc un groupe de travail sur l'intégration responsable dans l'écosystème du DNS, Blockchain, identificateurs et tout ce qui a un impact sur l'écosystème du DNS.

Et… Voilà, ce que vous avez donc à l'écran sur cette diapo. Donc, il y a tout un travail qui est effectué sur l'intégration et quels sont les risques qui existent lorsque vous travaillez dans ce domaine parce que c'est assez ouvert. Il y a différents opérateurs qui définissent de diverses manières ces points et qui dans certains cas, font des promesses. Et, je suppose qu'il y aura certains comportements qui vont survenir ou pas. Il n'y a pas de garantie à ce niveau. Il n'y a pas de cohérence.

Donc par exemple, un espace de noms qui n'est pas le DNS et vous voulez intégrer cet espace de nom n'étant pas le DNS dans le DNS, mais s'il n'y a pas d'intégration possible de liens entre les deux, cela ne va pas être possible. Et, donc, il va y avoir des problèmes qui vont survenir. Et vraiment… Nous en avons parlé lors de plusieurs séances plénières à l'ICANN.

Ce qui est fondamental ici, c'est que, comme toute technologie qui évolue rapidement et bien, on peut exprimer son identité différemment. Et lorsque l'on voit l'espace des noms de domaine, il y a une nomenclature qui existe, il y a des règles qui existent, des comportements attendus, il y a une confiance qui s'est établie après beaucoup de temps et lorsqu'on a un nouvel espace, et bien nous allons avoir cette question de la confiance qui va se poser. On parle de résolveur même si on ne parle pas de résolveur du DNS, on parle de nom de domaine, même si ce ne sont pas des noms de domaine dans le DNS. Donc, on utilise les mêmes noms parce que les noms ont été établis. La confiance a été établie dans le cadre de

ces noms, pour les utilisateurs, pour les entreprises dans le monde entier.

Mais il y a des risques qui existent. C'est que lorsque vous réutilisez donc non seulement les noms, mais lorsque vous prenez des parties, des fonctionnalités qui fonctionnent bien dans l'espace du DNS et que vous le marié avec d'autres fonctionnalités qui sont uniques à d'autres espaces de noms et que vous mélangez un petit peu les deux, et bien là vous pouvez avoir une grande confusion pour les utilisateurs. Quelle est mon identité? Quel est ce nom de domaine? Pourquoi ça ne fonctionne pas sur mon navigateur? Lorsque j'envoie un courriel et ainsi de suite, il y a des attentes. On s'attend à ce que cela fonctionne. Donc, on a besoin de plus de clarté à ce niveau. Donc ça, ce sont les premières étapes et nous allons avancer dans la présentation.

Et nous voyons qu'à court terme, nous nous concentrons sur l'impact sur la prochaine série de gTLD. Et nous avons noté que l'ICANN a donc un guide de candidature. Il y a de cela plusieurs mois ou même l'année dernière, nous avons fait un travail sur les collisions de noms et le conseil d'administration de l'ICANN l'a pris très au sérieux, l'a adopté, a adopté les recommandations et ICANN org met en œuvre ces recommandations. Mais, nous avons l'intention d'avoir un cadre de référence analytique pour la prochaine série de gTLD, parce que nous pensons que les utilisateurs pourraient connaître des problèmes avec des collisions, par exemple.

Je crois que tout n'avait pas été couvert dans notre rapport, donc on se concentre là-dessus maintenant et ce groupe de travail va gérer cela. Ce groupe de travail aura une séance à Prague à cette réunion de Prague, et nous allons entrer dans les détails si cela vous intéresse, joignez-vous à nous. Venez nous écouter dans nos délibérations. SSAC Je ne sais pas si vous avez des questions.

JONATHAN ZUCK

Tout d'abord, rapidement la collision des noms. En effet, ça nous concerne beaucoup à At-Large. C'est pour cela que nous avons une bonne collaboration. Et vous avez tiré la sonnette d'alarme à ce niveau. Ce n'est pas un niveau de doctorat, mais un niveau plus simple et cela nous concerne en effet. Donc, est-ce que vous élaborez des recommandations en temps et en heure, une méthodologie qui va arriver assez tôt ou c'est simplement une appel à la prudence que vous lancez?

Est-ce que vous pensez qu'il y aura une bonne manière de gérer cela parce qu'il y a déjà eu des promesses de faites? On essaie de faire une intégration très en douceur, une évaluation également. Donc je ne voudrais pas que cela soit mal interprété. Mais est-ce que vous allez être en mesure de nous dire exactement comment procéder?

WARREN KUMARI

Personnellement, je crois qu'il faut que les personnes soient bien au courant. Pour la dernière série, il y avait beaucoup de questions

sur les adresses courriel. Il n'y avait pas de procédure en place en temps et en heure et nous devons être prêts lorsque cela se passe, bien connaître les processus et les politiques.

Ce n'est pas une importance secondaire. C'est être prêt et que tout le monde soit informé également. Et lorsque cela se survient, qu'il y ait plusieurs applications qui proviennent de plusieurs fournisseurs de blockchain, voir à quel point c'est une priorité pour les utilisateurs finaux et s'assurer en tout cas qu'il y ait des processus qui soient bien compris.

RAM MOHAN Donc, je ne veux pas donc trop m'avancer puisqu'il y a un groupe de travail, mais je pense que, on va plutôt dire : Il va y avoir des dragons plutôt que de dire ça, c'est bien, ça, c'est pas bien.

JONATHAN ZUCK Oui, parce que, en effet, la nouvelle série arrive très prochainement.

JUSTINE CHEW Je crois que c'est très intéressant et nécessaire et je peux vous dire que de par mon expérience au forum du DNS de l'APAC, je crois que vous étiez présents. Eh bien, on a exprimé clairement une confiance que le Web.3 va arriver très rapidement. C'est l'expression dont je me souviens que ça va changer. Les choses

vont changer. C'est une préoccupation véritable, cette évolution du Web.

Et ils vont utiliser les chaînes différemment, dans un espace différent. Et ça va être comme cela qu'il faut obtenir les chaînes. Il n'y aura plus de candidatures pour obtenir des chaînes, donc il faut être très prudent à ce niveau et être très attentif et vigilant. Le conseil d'administration doit suivre ses ramifications et conséquences de près.

Les tactiques des acteurs du Web3, c'est beaucoup de jargon que l'on ne comprend pas. Donc ils nous disent : Web2 devrait apprendre de Web3. Et c'est quoi Web2? Il n'y a que le web et donc Web3, ce n'est pas pratique pour tout l'internet. Donc personne ne comprend bien ces concepts, mais ils lancent en l'air des noms Web3 et ainsi de suite. C'est très préoccupant tout cela.

RAM MOHAN

Merci beaucoup. Nous sommes conscients de cela. Le temps s'écoule. La prochaine série arrive bientôt. Le groupe de travail se réoriente et se concentre plus précisément sur ces problématiques et sur des aspects plus spécifiques, des conseils plus spécifiques et des commentaires qui peuvent être pris en compte en effet par l'ICANN pour prendre cela en compte dans le guide de candidature. Donc, nous avons conclu notre travail avec la collision de noms et cette partie en fait. C'est un petit peu quelque chose qui est en suspens.

Diapo suivante. Nous allons voir le dernier travail que nous faisons. Donc les considérations opérationnelles pour le DNSSEC. Eh bien, fondamentalement, ce qu'on essaie de résoudre, c'est que le DNSSEC, comme vous le savez, existe depuis pas mal de temps, mais ce n'est pas un succès du jour au lendemain que nous avons connu.

Et pourquoi n'est-il pas plus utilisé, le DNSSEC? Et quels sont les obstacles? Quelles sont les solutions pratiques que l'on peut trouver pour le DNSSEC pour qu'il soit au niveau opérationnel? Et ce qui est assez compris, ce DNSSEC. Donc voilà ce que nous essayons de faire. C'est un groupe de travail qui va se réunir également ici à la réunion de Prague, et vous pouvez le trouver sur l'ordre du jour de notre réunion de Prague.

Et voilà, je crois que nous sommes à la prochaine diapo. Jonathan, ensemble, nous parlions de cela lors de la dernière réunion et même celle qui a précédé. Donc, si vous restez donc sur cette diapo, les prochaines étapes pour cette campagne de cybersécurité, c'est Safer Cyber. Et bien c'est quelque chose que vous avez bâti, dont on parle maintenant, qui est disséminé un peu partout et c'est très encourageant. Nous venons vous voir et nous voulons lancer un dialogue maintenant et à l'avenir pour vous, cette initiative de cybersécurité et d'avoir un espace cybernétique plus sûr.

Donc, ce que nous voulons faire avec vous ici et en ligne, c'est de voir ce qui serait intéressant comme question, comme

problématique pour votre public. Je crois que nous avons des documents qui ne sont pas exactement écrits pour les utilisateurs finaux, mais il y a des documents intéressants SAC40 et d'autres documents également pour les deux sujets proposés, les deux thématiques proposées. Nous avons beaucoup de rapports qui existent, qui vont être utilisés. Donc c'est ouvert. Je laisse cela ouvert. Qu'est-ce qui vous intéresse le plus et comment est-ce que nous pourrions progresser à ce niveau?

JONATHAN ZUCK

Je donne à tout le monde la possibilité de s'exprimer et je crois que c'est tout à fait positif. Et c'est un nouveau groupe que Amrita préside et ça va être le conduit de ces conversations. Et nous avons quelques personnes et également nous avons des espions ou espionnes SSAC qui nous informent et c'est tout à fait intéressant.

Je crois que nous voudrions avoir un pipeline en effet, de thématiques de ce type, parce que nous avons besoin d'alliances plus fortes avec nos ALS, des collaborations avec des bibliothèques. Donc ça va être toujours quelque chose qui va être poursuivi. On peut personnaliser, je pense, peut-être un petit peu ces points et voir comment on peut disséminer ces informations. Je crois qu'on a besoin de financement parfois pour ce faire, à moins que l'on produise nous-mêmes ces documents. Mais c'est intéressant. Continuons donc notre travail. Voyons le programme de subvention comme mécanisme éventuel pour continuer le travail que fait SSAC et le faire connaître. Je crois qu'il y a des fonds

disponibles et qu'on pourrait les utiliser de cette manière. Donc continuons les débats. Il ne reste que deux minutes, je crois. Et je pense que c'est une bonne idée, en tout cas ce que vous avez proposé.

Est-ce qu'il y a des questions ou des commentaires pour Ram? Je ne vois pas la liste des participants en ligne. Je ne vois pas s'il y a des mains levées. De toute façon, je pense qu'il est temps de clore la séance. Mais on aime tellement nos réunions conjointes ALAC-SSAC que ça y est, on est arrivé à la fin de cette réunion et il faut demander à l'ICANN d'organiser une retraite, une retraite de trois jours consacrée à voir comment est-ce qu'on peut faire en sorte que les utilisateurs soient plus sûrs en ligne. Voilà pour le prochain cycle budgétaire proposant cela.

Bref, blague à part, merci à tous d'être venus. On apprécie toujours que vous veniez nous voir. Et maintenant, la communication est ouverte entre nous.

RAM MOHAN Merci à vous.

[FIN DE LA TRANSCRIPTION]