ICANN74 | Forum de politiques – Séance sur les politiques d'At-Large 1 : faire évoluer la conversation sur l'utilisation malveillante du DNS : perspective de l'utilisateur final - le rôle de l'At-Large
Lundi 13 juin 2022 – 15h00 à 16h00 AMS

YESIM SAGLAM: Veuillez s'il vous plait prendre place dans la salle, nous allons commencer d'ici peu. Merci. La séance va maintenant commencer, lancez l'enregistrement.

Bonjour et bienvenue à la séance politique At-Large, faire évoluer la discussion sur l'utilisation malveillante du DNS, le point de vue de l'utilisateur finale et le rôle d'At-Large.

Je m'appelle Yesim Saglam et je suis responsable de la participation à distance pour cette séance. Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendues de l'ICANN.

Veuillez noter que pendant cette séance les questions et les commentaires soumis dans le chat seront lus à haute voix s'ils sont soumis dans le bon format, tel que noté dans le chat. Si vous êtes à distance, attendez qu'on vous appelle par votre nom et activez votre micro sur Zoom.

Pour ceux d'entre vous qui sont ici en salle, veuillez lever la main sur Zoom et lorsqu'on vous appellera veuillez activer votre micro

sur votre table. Dans la salle secondaire, veuillez lever la main sur Zoom et aller vers le micro volant lorsqu'on vous appellera par votre nom.

Pour le bénéfice des autres participants, veuillez indiquer votre nom pour l'enregistrement et parler à un rythme raisonnable.

Les participants sur place pourront prendre un récepteur et utiliser leurs propres écouteurs pour suivre l'interprétation. Les participants à distance peuvent accéder à l'interprétation à travers la barre d'outils de Zoom.

Je vais à présent céder la parole à Hadia Elminiawi.

HADIA ELMINIAWI: Merci beaucoup. Bienvenue à tous à cette séance politique d'At-Large sur le rôle d'At-Large dans l'atténuation de l'utilisation malveillante du DNS, les activités malveillantes sur internet avec des noms de domaine enregistrés à des fins malveillantes. Dans cette séance on va se concentrer sur le rôle des RALO dans l'organisation et organiser la communauté pour essayer d'atténuer l'utilisation malveillante du DNS.

Nous avons un certain nombre des membres du panel qui vont un petit peu planter le décor, orienter nos discussions. Toutefois nous aimerions que cette séance soit aussi interactive que

possible. Donc surtout n'hésitez pas à lever la main pour nous faire part de votre opinion. Il s'agit des RALO et de ce que les RALO doivent faire pour avancer.

Je vais commencer par Léon Sanchez, le vice-président du conseil d'administration de l'ICANN. Bienvenue Léon et merci de nous accompagner aujourd'hui. Pourriez-vous, s'il vous plait Léon, nous parler des défis auxquels la communauté est confrontée ?

LÉON SANCHEZ: Oui, merci beaucoup Hadia. Tout d'abord merci de m'avoir invité à cette séance si importante. Alors, par où commencer ?

Parce que les défis auxquels la communauté est confrontée en termes d'utilisation malveillante du DNS sont nombreux, à commencer par la discussion sur la manière dont nous comprenons, dont nous définissons l'utilisation malveillante du DNS. Ça, c'est le principal défi, n'est-ce pas, pour commencer.

Nous avons quelques définitions dans nos statuts constitutifs par rapport à l'utilisation malveillante du DNS, des orientations par rapport à ce qu'on pourrait considérer être une utilisation malveillante du DNS, mais là encore il y a des conduites, des comportements, des situations qui pourraient ne pas être aussi tranchées que cela pour qu'on puisse les considérer d'entrée comme une utilisation malveillante du DNS.

Donc d'abord comment définir l'utilisation malveillante du DNS. Et, à cela s'ajoutent – c'est une autre couche – les différentes approches, les différents intérêts qu'ont les différentes parties prenantes au sein de cette discussion.

Donc je pense qu'une fois encore les différents défis sont les suivants : comment trouver une définition, voire réfléchir au fait de savoir si on veut vraiment définir cela. Parce que si on définit cela, on reste attaché pour l'avenir à cette définition. Peut-être qu'il faudrait éviter un manque de souplesse si on crée une définition qui découlerait de la discussion. Et il est important d'insister sur le fait que la définition doit venir de la communauté et non pas du conseil d'administration ou de l'organisation ICANN, parce que sinon cela ne relèverait pas et ne serait pas propre de notre processus multipartite ascendant.

C'est pourquoi je pense qu'il est important que du point de vue du conseil d'administration on fasse notre possible pour faciliter cette discussion, ce dialogue, et qu'on encourage le fait de réunir les conditions qui vont permettre à la communauté de débattre de cette question et que chaque partie de la communauté comprenne bien les différents niveaux qui interviennent dans cette utilisation malveillante du DNS.

Et, encore une fois, cette séance témoigne bien des efforts qui sont déployés au sein de la communauté At-Large pour essayer de

régler cette question de l'utilisation malveillante du DNS. Il y a d'autres efforts déployés au sein de la GNSO, de la ccNSO qui vont dans le même sens. Et le défi ici, encore une fois, c'est d'essayer de trouver le bon équilibre et les bonnes synergies, le bon rythme, pour essayer de faire en sorte qu'on ait une compréhension commune autour de l'utilisation malveillante du DNS.

Donc je pense que c'est le principal défi.

Pour ma part je suis convaincu que le conseil d'administration devrait jouer un rôle de facilitateur qui rallierait un petit peu la communauté autour d'une compréhension commune.

Mais, en tout cas, en l'état actuel des choses, ce rôle devrait se limiter à cela.

HADIA ELMINIAWI: Merci, Léon, de cela. Alors vous avez parlé de différentes approches et différents intérêts. Alors, comment nous voyez-vous, en tant que communauté, pour nous organiser et travailler ensemble vers un objectif commun ? Il y a, vous l'avez dit, un certain nombre d'initiatives au sein de la communauté qui impliquent toute une série de parties prenantes, mais comment travailler tous ensemble plutôt que d'avoir des initiatives isolées qui sont développées en parallèle ?

LÉON SANCHEZ: Merci, Hadia. Je pense que l'une des grandes forces que nous avons en tant que communauté c'est précisément notre diversité. Et, en tant que tel, je ne vois pas d'efforts parallèles comme étant un obstacle, une entrave. Je pense au contraire que des efforts parallèles peuvent finalement donner lieu à un effort collectif. Donc moi, ce que je préconiserais, c'est que l'on participe tous à ces efforts parallèles, qu'on suive ces efforts et qu'on essaye tous de contribuer à cet effort.

Et je pense qu'en fin de compte tous ces efforts vont converger vers une voie unique. Et tous les efforts parallèles vont finalement alimenter un effort commun qui va nous permettre de pouvoir parvenir à une définition commune ou à une compréhension commune de ce que serait ou non l'utilisation malveillante du DNS.

Alors ce qui serait contre-productif, pour moi, si je vous disais de faire ceci ou de ne pas faire cela. Non, ça n'est pas ce que je vais faire. La grande force c'est qu'on ait beaucoup d'efforts déployés autour de cette question pour finalement trouver un moyen de combiner les points de vue et de faire en sorte que tous les résultats de ces processus parallèles donnent lieu à un effort plus large, vigoureux, qui englobe toute la communauté. Et avancer d'une manière qui soit bénéfique pour toute la communauté.

HADIA ELMINIAWI: Merci, Léon. Est-ce que vous pourriez nous dire quelques mots par rapport aux efforts réalisés dans ce sens ?

LÉON SANCHEZ: Vous voulez dire les efforts qui sont réalisés par exemple du côté de la communauté ? Écoutez, le conseil d'administration est en train de discuter de cette question aussi. Comme vous l'avez dit, il y a des efforts et des pistes qui ont lieu en ce moment. Et l'une de ces pistes est explorée au niveau du conseil d'administration. On a eu des discussions pour voir comment aborder ce défi qui consiste à essayer d'avoir une compréhension commune ou de définir l'utilisation malveillante du DNS lors de notre atelier de travail qui s'est fini dimanche dernier, donc hier. Mais là encore, ça fait partie de nos préoccupations et priorités parce qu'on sait que c'est important pour l'organisation et pour la communauté aussi. Donc on en parle.

Maintenant, s'agissant des efforts de l'organisation ICANN, je peux vous dire qu'il y a de nombreux efforts entrepris pour essayer d'aborder la question de l'utilisation malveillante du DNS qui varie d'un point de vue technique à un point de vue et une approche un peu plus pragmatique pour faciliter les discussions pour essayer de combler les fossés par rapport à ceux qui ne

respectent pas les termes et dispositions du contrat. Donc, effectivement, il y a des efforts déployés au niveau de l'organisation et du conseil d'administration – et je vous invite à les suivre – pour alimenter ce processus. Parce qu'il est important que l'on connaisse votre point de vue et que l'on puisse l'intégrer dans ces efforts.

HADIA ELMINIAWI: Merci beaucoup. On attend avec impatience de pouvoir participer à vos efforts. Je me tourne vers Joanna, pourriez-vous résumer pour nous les activités At-Large par rapport à l'utilisation malveillante du DNS.

JOANNA KULESZA: Merci beaucoup. Et veuillez noter qu'on m'a donné 7 minutes pour résumer la kyrielle d'activités qui ont lieu au sein d'At-Large par rapport à l'utilisation malveillante du DNS. Un grand défi.

Donc je reprends à mon compte ce qu'a dit Léon, à savoir que cette question de l'utilisation malveillante du DNS est si vaste que d'un côté c'est difficile de l'aborder en tant que question politique, mais d'un autre côté, ça déclenche toute une série d'autres discussions politiques ; et j'aimerais aborder les choses de ce point de vue là. Nous, à At-Large, nous avons abordé l'utilisation malveillante du DNS comme une question prioritaire

pour la discussion de la communauté lors de nos réunions présentielles, nos dernières réunions présentielles.

Et, donc, nous avons organisé sur cette thématique de l'utilisation malveillante du DNS pendant les forums publics et réunions publiques qu'on a eus à Kobe, par exemple, ce genre de discussions avec les représentants de la communauté, représentants des autres unités constitutives, Graeme inclus – merci de votre présence aujourd'hui – et on a toujours soutenu cette ligne avec un certain nombre d'initiatives.

D'ailleurs, s'agissant de sensibilisation et d'engagement nous avons a=organisé une série de webinaires de renforcement de capacité qui ont pu être organisés grâce au soutien de Hadia qui a été le grand moteur derrière toutes ces initiatives qui se concentrent sur l'utilisation malveillante du DNS. Donc on a sensibilisé par rapport à ce que pourrait être l'utilisation malveillante du DNS avec des réunions en ligne, mais aussi des webinaires visant à offrir des informations complètes sur l'utilisation malveillante du DNS. Mais en raison de la pandémie, on a dû réduire le nombre de mesures qu'on pouvait entreprendre à ce niveau-là. Mais l'important c'était d'organiser cette discussion et surtout présenter à la communauté At-Large plus large un récit assez cohérent par rapport à l'utilisation malveillante du DNS.

Nous passons maintenant aux politiques et en ce qui les concerne l'utilisation malveillante du DNS est un sujet constamment présent. Nous avons un positionnement pour l'utilisation malveillante du DNS au sein du groupe de travail sur les politiques consolidées, et je suis impatiente d'entendre Olivier qui nous parlera des détails dans ce domaine. L'utilisation malveillante du DNS n'est pas pour l'instant un sujet de politique pour l'ICANN par rapport aux SubPro ou à l'acceptation universelle. Cela veut dire que nous ne pouvons pas de manière officielle fournir notre feedback. Donc l'utilisation malveillante du DNS et toutes ces questions demandent à ce qu'on invite des personnes également extérieures à la communauté, mais pour l'instant nous n'avons pas formé de groupe de travail consacré, de petites équipes consacrées qui puissent s'occuper de ces questions d'abus du DNS.

Certes, ceci ressort dans différents sujets sur les politiques et At-Large cherche les opportunités de donner la perspective des utilisateurs finaux dans le cadre des processus d'élaboration des politiques et des avis.

Ceci étant, c'est un réseau d'entreprises, d'initiatives qui ont lieu et qui incluent d'autres acteurs externes. Mais ce n'est pas une opportunité unique pour nous de participer. Il semblerait qu'il y a davantage d'opportunités de parler de l'utilisation malveillante

du DNS en dehors de la communauté de l'ICANN également. C'est un sujet constant pour la collaboration bilatérale entre l'At-Large et le GAC, il y a un petit groupe plus restreint qui se concentre sur les rapports de la Commission européenne dans l'objectif d'élaborer la perspective sur les politiques à ce sujet. Ce petit groupe a organisé une réunion juste avant l'ICANN 74 et donc nous espérons rapidement entendre ce dont ils ont parlé.

Donc il faut renforcer les capacités, il faut élargir le networking. Nous savons bien qu'il y a des intérêts supérieurs, c'est quelque chose qui est technique, qui nécessite davantage d'informations. En ce qui concerne les politiques, il faudrait que les choses soient très claires du point de vue de l'At-Large.

Nous n'avons pas identifié de besoins de mettre en place un petit groupe de travail, mais c'est quelque chose qu'on pourrait faire. Et je repasserai la parole à Hadia pour qu'elle nous dise quelles sont les opportunités.

Donc ces éléments pour moi sont une démarche complète de l'At-Large en ce qui concerne l'utilisation malveillante du DNS et je serais curieuse d'écouter les intervenants suivants. Merci.

HADIA ELMINIAWI : Merci beaucoup, Joanna. Ceci nous permet maintenant de parler avec les RALO de connaitre le rôle qu'elles ont pour atténuer

l'utilisation malveillante du DNS. Je vais commencer par AFRALO. Seun ? Je crois que Seun est en ligne.

SEUN OJEDEJI : Oui, je suis là, j'espère que vous m'entendez.

HADIA ELMINIAWI: Oui, merci d'être là avec nous. Donc quel est le rôle, selon vous d'AFRALO, pour contribuer à l'atténuation de l'utilisation malveillante du DNS.

SEUN OJEDEJI : En ce qui nous concerne, il y a une chose qu'il faut noter, c'est que nos membres sont des utilisateurs finaux typiques. La seule chose qu'ils font c'est qu'ils vont en ligne, qu'ils cliquent sur un lien et ils veulent obtenir le résultat attendu.

Donc, à AFRALO, je crois que certaines choses que l'on pourrait faire et que pour certaines nous avons faites, c'est de sensibiliser et renforcer les capacités. Je crois qu'il est très important de noter qu'en principe nous avons des séries, des séries sur ces sujets et donc ces séries se concentrent parfois sur l'utilisation malveillante du DNS. Et, de temps à autre, nous avons des déclarations, par exemple la déclaration pour l'ICANN 74 qui sera faite mercredi, donc dans ces déclarations nous parlons souvent

de l'utilisation malveillante du DNS au sein de la communauté de l'ICANN et au sein d'AFRALO.

Donc, personnellement, je pense que la sensibilisation, le renforcement des capacités c'est ce que nous pouvons faire en tant que RALO. Comment davantage informer nos membres et les sensibiliser de manière à ce qu'ils puissent mieux utiliser l'internet avec leurs connaissances souvent limitées.

Mais, comme cela a été déjà noté, je crois l'important c'est de contribuer au sein de l'ICANN à tout ce qui est relatif à l'utilisation malveillante du DNS. Donc lorsque nous renforçons les capacités au sein d'AFRALO comment ce feedback informe un système existant au sein de l'ICANN.

Il serait également bon de travailler dans ce sens, et je crois que cela a été dit tout à l'heure. Donc on pourrait peut-être faire des progrès dans ce sens de manière à ce qu'il y ait un moyen de communiquer le feedback des RALO aux groupes de travail et l'idée étant d'obtenir des résultats qui pourraient être acceptés de manière générale dans le contexte de l'ICANN.

Donc pour nous, pour AFRALO, nous allons continuer de sensibiliser et bien sûr nous allons continuer de renforcer les capacités et lorsque nous avons l'opportunité de contribuer aux sujets de politique relatifs à l'utilisation malveillante du DNS nous

continuerons d'encourager nos membres à agir dans ce sens. Merci.

HADIA ELMINIAWI : Nous avons un commentaire, je vais donc passer la parole à Yesim.

YESIM SAGLAM: Merci beaucoup, Hadia. Nous avons un commentaire de Naveed Bin Raise. Il nous dit : il semble que l'utilisation malveillante du DNS a été acceptée par la communauté comme problème mais nous n'avons toujours que très peu de consensus au sein de la communauté sur sa correspondance avec la mission de l'ICANN. Il y a différentes parties de la communauté qui considèrent différentes perspectives de l'utilisation malveillante du DNS et il faut arriver à un consensus communautaire sur la définition de l'utilisation malveillante du DNS avant de pouvoir réellement atténuer le problème.

HADIA ELMINIAWI: Merci, Yesim. Je ne sais si quelqu'un souhaite faire un commentaire par rapport à ça, mais personnellement je pense qu'il n'est pas nécessaire d'attendre avant d'atteindre le consensus à ce sujet pour atténuer, commencer à atténuer. Je

crois qu'il faut commencer à s'attaquer au problème. Comme cela a été dit, le problème est là, c'est suffisamment motivant, je crois, pour essayer de voir comment solutionner le problème. Et je crois que du point de vue de l'At-Large c'est une perspective importante parce que cela a un impact sur la sécurité des utilisateurs finaux de l'internet et cela a un impact sur leur confiance. Il y a une organisation qui a beaucoup de points dans l'internet et c'est l'ICANN.

Je ne sais pas si quelqu'un souhaite faire un commentaire là-dessus ?

JOANNA KULESZA: J'aimerais dire quelque chose. Le problème est noté, c'est vrai, il est difficile d'identifier ce qui fait vraiment partie de la mission, mais en même temps cela fait partie du problème et de la solution, parce que c'est aussi global et aussi large en termes de compréhension. Et donc il y a une opportunité pour l'At-Large de contacter la communauté, d'entrer en lien pour vraiment comprendre quels sont les différents aspects de l'abus du DNS. Mais j'ai hâte d'entendre les autres intervenants parce que je pense que les personnes qui travaillent vraiment sur le terrain auront des réponses un peu plus spécifiques à apporter à cette question. Merci.

GRAEME BUNTON : Je suis Graeme du DNS Abuse Institute. J'ai quelque chose à dire sur la discussion sur la définition et je suis d'accord avec Hadia, sur ce point. Il n'est pas nécessaire d'en arriver à un point de consensus sur une définition totale de l'abus du DNS pour avancer. Et d'ailleurs je vais insister parce que je crois qu'il est très facile de passer beaucoup de temps à parler de tout ce qui est un petit peu en marge de l'abus du DNS, mais faire le travail pour atténuer c'est beaucoup plus difficile. Et donc pour cette communauté, surtout dans le contexte de la discussion sur la collaboration, je crois qu'il faut se concentrer sur les lieux où nous sommes d'accord et commencer à vraiment attaquer l'abus du DNS.

Je pense qu'il y a un accord relativement général, tout ce qui est hameçonnage, les programmes malveillants et autres domaines, nous sommes d'accord là-dessus.

Donc trouver des moyens de faire des progrès là-dessus c'est déjà une bonne chose, ainsi que les réseaux zombie. Donc je crois que cela peut apporter une certaine valeur.

Alors, si on se met à réfléchir à tous les éléments de définition sur l'utilisation malveillante du DNS, il sera difficile d'inclure certaines choses très spécifiques. Nous parlons assez rapidement

dans cette communauté, parce que c'est pratique et relativement clair, mais pour cette question, je crois qu'il faut partir de manière assez large. Pourquoi est-ce que tout ceci doit être atténué au niveau du DNS ? Et je crois que la question de la définition est complexe. Mettons ceci de côté, concentrons-nous sur les lieux où il y a consensus et avançons. Merci.

HADIA ELMINIAWI: Merci Graeme. Et je passe maintenant la parole à APRALO. Satish ? Si vous voulez bien nous dire ce que vous pensez du rôle d'APRALO dans l'atténuation de l'abus du DNS.

SATISH BABU: Merci Hadia, merci pour cette opportunité, donc. Je sais que ce n'est pas quelque chose dont on a beaucoup parlé dans la région, donc c'est mon opinion personnelle que je vais vous donner et je ne suis pas expert.

Alors, je crois que la sécurité ce n'est pas une définition mais c'est un chemin. Ce qui est nocif, actuellement, pourra ne pas être nocif à l'avenir. Donc on ne peut pas avoir de définition fixe. Je pense qu'essayer de définir cela dans les statuts me surprend, je pense que c'est trop complexe. Donc nous pouvons commencer et ensuite, avec le temps, la GNSO, la ccNSO, le conseil

d'administration pourront affiner ceci sur la base des différents préjudices qui se présenteront.

Alors, Seun a déjà parlé de renforcement de capacité, de sensibilisation, je suis tout à fait d'accord, c'est la base. Mais j'irai un petit peu plus loin, je parlerais de plaidoyers au niveau des organisations locales, des autorités locales. Et, enfin, les outils et les technologies. Nous avons entendu parler de NetBeacon, nous avons parlé de l'utilisation de l'intelligence artificielle, nous avons le DNS Abuse Institute, donc nous devons continuer de collaborer avec tout ceci. Et puis il nous faudrait un groupe permanent, comme Joanna l'a dit, je suis d'accord.

Est-ce que nous pourrions peut-être avoir une sorte de surveillance qui soit mise en place au niveau des RALO ? Parce que c'est quelque chose qui affecte tout le monde, c'est un petit peu comme une catastrophe naturelle. Lorsqu'on a eu la Covid, lorsqu'on a d'autres choses qui se passent ceci est utile. Donc est-ce qu'on pourrait peut-être penser à un système de surveillance inter-RALO qui nous permette de surveiller ce qu'il se passe dans cet espace ? Et puis, avec le temps, on peut toujours faire évoluer ceci, mais je crois qu'il est plus facile de coordonner des actions au niveau de la communauté de l'At-Large, qui est très répandue, lorsqu'on a des points de travail commun.

HADIA ELMINIAWI: Merci, Satish. Oui, effectivement, At-Large a cette voix mondiale et on doit l'utiliser. Et c'est l'une des raisons pour lesquelles nous avons cette conversation aujourd'hui.

Vous avez également parlé des technologies et là encore je pense que c'est un aspect très important. Jusqu'à présent je ne pense pas qu'At-Large ait beaucoup utilisé les technologies dans ce sens, que ce soit par rapport au fait de notifier de cas de fraudes ou d'assurer un suivi.

Je vais maintenant passer à EURALO. Je crois qu'Olivier est avec nous en ligne, oui ? Merci Olivier de nous accompagner. Alors, quel est le rôle d'après vous d'EURALO ? Et je sais que vous allez également nous parler d'un outil.

OLIVIER CREPIN-LEBLOND : Merci beaucoup Hadia, j'espère que vous m'entendez bien parce que je crois que le son de mon micro n'est pas assez élevé.

YESIM SAGLAM: Allez-y.

OLIVIER CREPIN-LEBLOND : Très bien, merci. Je vais essayer de parler plus fort.

Alors l'utilisation malveillante du DNS est intéressante, et là je vais mettre deux casquettes. La première, vous avez parlé d'abord du groupe de travail sur la politique consolidée ; il s'agit effectivement d'un groupe qui traite de toutes les questions politiques à At-Large, il y a un certain nombre de positions qui ont été fixées au sein de ce groupe, un certain nombre de déclarations ont été envoyées à l'ICANN sur toute une série de recommandations. Et un dialogue qui a lieu en ce moment entre l'ALAC et le conseil d'administration qui a été élaboré par le groupe de travail sur les politiques consolidées et ratifiées par l'ALAC sur toutes ces questions. Donc c'est intéressant d'avoir un dialogue entre le conseil d'administration et notre partie de la communauté.

Mais il n'en demeure pas moins qu'on est encore coincés sur cette question : comment définir l'abus du DNS ? Et on s'aperçoit que la discussion devient tellement [inaudible] qu'il est inutile de définir quelque chose pour lutter contre cette chose, parce qu'il suffit de connaitre cette chose, inutile de la définir pour lutter contre elle. Et c'est intéressant parce que certaines de nos ALS, à EURALO, et là j'ai une autre casquette, ISOC Belgique, a dit : écoutez, oubliez cette définition mais faisons quelque chose pour lutter contre l'abus du DNS. Et ils ont créé [IsTrust]. Il s'agit de noms de domaine et de confiance dans ce nom de domaine et du site web

auquel ces noms de domaine appartiennent, que ce soit un add-one sur votre navigateur, ça fonctionne sur Firefox comme sur Edge, il suffit de télécharger un petit badge sur lequel vous cliquez et cela vous donnera le niveau de fiabilité sur le site web, où il a été enregistré, à qui il appartient et tout ce qui concerne les fournisseurs de la communication autour de ce site web. ISTRUST.ORG, voilà le site web en question. C'est un outil gratuit, open source, vous verrez que c'est tout à fait fiable, rien du type accaparement de vos données personnelles. Et donc on voit que c'est intéressant parce que les structures et At-Large en général vont dans cette direction. Et ceux qui ont une mission technique nous montrent bien qu'on va avoir de plus en plus d'outils de ce genre qui vont surgir, qui vont pousser Graeme et son institut à travailler plus dans ce sens.

HADIA ELMINIAWI : Merci Olivier. Alors oui effectivement, il faut utiliser les technologies qui sont à notre disposition. Je passe maintenant… Je sais que nous avons une main levée sur Zoom. Avons une main levée, Yesim ?

YESIM SAGLAM: Oui, merci Hadia. Nous avons deux mains levées sur Zoom, premièrement Carlos Dionisio et deuxième main Daniel Nanghaka. Merci.

HADIA ELMINIAWI: Carlos, allez-y.

CARLOS DIONISIO: Merci Hadia. Je vais m'exprimer en espagnol. Écoutez, je crois que ça a été très bien dit, à l'instant Graeme vient d'évoquer l'inutilité de définir, il ne s'agit pas de définir ici le problème mais plutôt d'instaurer le problème et cette discussion dans la société et de dire qu'on a déjà un consensus minimum, à savoir que c'est un fléau. C'est un fléau qui nous fait du mal. Donc pour rallier plus de gens dans cette discussion, comme vous l'évoquiez à l'instant, Hadia, on a besoin que chaque fois plus de membres de la communauté et d'utilisateurs finaux individuels puissent nous donner leur point de vue sur toutes ces questions et voir comment nous aider, nous, à trouver des solutions.

Donc je pense qu'il faudrait travailler davantage sur la diffusion, le fait de se rapprocher des différentes parties de la communauté pour éclairer, informer. Non seulement au sein de la communauté ICANN, mais au-delà, dans les cercles académiques, universitaires et autre.

Donc c'est un travail énorme que l'institut sur l'utilisation malveillante du DNS – d'ailleurs j'en profite pour féliciter Graeme pour l'excellent travail – donc c'est un rôle qu'a déjà l'institut sur l'utilisation malveillante du DNS, mais je pense que nous aussi, nous devrions participer à ce niveau-là.

HADIA ELMINIAWI: Merci, Carlos de votre intervention. On va passer à la deuxième demande d'intervention.

DANIEL NANGHAKA: J'espère qu'on m'entend bien. Sur les questions liées à l'utilisation du DNS, je pense que cela requiert une approche multipartite. D'abord, la question de la communauté technique, elle doit s'assurer qu'ils font une bonne mise en œuvre des outils dans leur juridiction respective. Les noms de domaine ne peuvent pas faire l'objet d'abus.

Maintenant s'agissant des utilisateurs finaux, nous à At-Large, avons un rôle important à jouer. Et je pense qu'on a vu qu'il y a beaucoup de webinaires qui ont été organisés sur l'utilisation malveillante du DNS, on a vu des ALS organiser des activités au sein de leur communauté, mais s'agissant de la mise en œuvre politique, là je pense qu'il faut combler le fossé par rapport aux utilisateurs finaux. Quelles sont les choses qu'ils retiennent par

rapport à l'utilisation malveillante du DNS. D'abord ils ne comprennent pas forcément toute cette technologie, des outils qu'on pourrait tester en termes d'un sondage de spams pour pouvoir convaincre les utilisateurs finaux.

Deuxième point, pour ajuster une politique en vue de la mise en œuvre d'une politique dans le domaine de l'utilisation du DNS sur les sites web. En tant qu'At-Large, on pourrait parler aux techniciens et aux membres des groupes de travail techniques pour dire que ces outils sont obligatoires, qu'il faut absolument les utiliser. Peut-être que cela va représenter des frais supplémentaires, mais il est important de le faire.

HADIA ELMINIAWI : Merci beaucoup, Daniel, de votre intervention. Nous passons maintenant à LACRALO. Augusto ?

AUGUSTO HO : Merci beaucoup. Je vais m'exprimer moi aussi en espagnol. J'écoutais les échanges cet après-midi, pour essayer de trouver une définition unique ou faisant l'objet d'un consensus quant à l'utilisation malveillante du DNS.

Mais moi, j'aimerais parler du besoin des utilisateurs finaux. Et là je parle non seulement en tant que président de LACRALO mais comme professeur d'université et employé du secteur privé.

En décembre, dans mon pays le Panama, on a mis en place une nouvelle figure juridique, société d'entrepreneuriat. Et ce terme entrepreneuriat a pris de l'envergure ces deux dernières années, depuis que tant de personnes ont perdu leur emploi. Beaucoup de ces personnes se sont lancées dans des activités commerciales pour leur compte.

Et donc je recevais des témoignages des personnes de la région où on comprend que ces personnes qui se sont lancées dans des activités commerciales sont finalement devenues les nouvelles victimes de l'utilisation malveillante du DNS. Ce n'est plus comme ça a été le cas par le passé les grandes entreprises et leurs grandes marques dont le nom a été utilisé à mauvais escient. Ne perdons pas de vue que nous, les avocats, nous avons une intuition pour détecter les choses qui fonctionnent mal.

En tout cas, les entrepreneurs ont une grande quantité d'idées, mettent en œuvre un certain nombre d'initiatives, et on l'a vu, sont devenus le grand moteur de l'économie, on l'a vu pendant la pandémie. Et moi, je vous invite à réfléchir parce qu'au sein des utilisateurs finaux du réseau on a vu que ce sont eux, les autoentrepreneurs, qui sont finalement les plus touchés. Et ce

devrait être eux qui reçoivent le fruit de tout ce dont on parle ici.

On a dit ce matin que l'utilisation malveillante du DNS ça n'est pas une question abstraite, je retiens ce message. Je retiens également l'idée selon laquelle on doit agir en notifiant, en signalant. Et je pense que c'est important pour mettre en œuvre des solutions pour les personnes qui sont directement ou indirectement affectées par cette utilisation malveillante du DNS.

Merci.

HADIA ELMINIAWI: Merci beaucoup, Augusto. Et j'apprécie beaucoup votre idée par rapport au fait d'utiliser, de tirer partie des idées des autoentrepreneurs pour lutter contre l'utilisation malveillante du DNS. Donc, d'après vous, comment At-Large pourrait canaliser toutes ces idées, peut-être d'ailleurs que c'est plus que des idées, ça va plus loin, et les utiliser ces idées ?

AUGUSTO HO : Moi je viens vous dire qu'il faut former à un outil très important. Les entrepreneurs sont des gens qui se lancent dans une activité commerciale, d'accord, mais qui sont avides d'en apprendre plus sur une nouvelle activité. 75 à 80 % du développement

économique qu'on voit actuellement provient des entrepreneurs. À cela s'ajoutent les PME. Et donc on pourrait former ces personnes, on pourrait les former pour que ces personnes sachent comment compléter un formulaire de signalement d'incident. Les former dans le domaine de la propriété intellectuelle. Parce que tous ces entrepreneurs contribuent au développement économique mondial et apportent beaucoup plus qu'on ne peut l'imaginer. Et c'est tout un secteur de la situation qui mériterait beaucoup plus d'attention de notre part, parce que là, elles apportent non seulement au niveau économique mais également au niveau des idées, des idées qui sont très importantes au niveau de la propriété intellectuelle. Par rapport aux noms de domaine aussi.

Merci beaucoup.

HADIA ELMINIAWI: Merci beaucoup. Nous avons Léon qui a levé la main. Léon, allez-y.

LÉON SANCHEZ: Merci beaucoup, Hadia. Je parle en espagnol, à la suite de mes amis de la région. J'espère que tout le monde a ses écouteurs.

Je pense qu'il y a quelque chose d'important à souligner ici. Comme le disait Carlos à l'instant, et Graeme l'a dit aussi, s'il y a bien une chose sur laquelle on est d'accord, c'est qu'on n'a pas de définition et d'ailleurs on n'a pas besoin probablement de définition de ce que serait l'utilisation malveillante du DNS. Mais en aucun cas ça doit empêcher l'organisation ICANN de lutter activement contre ce que l'on connait communément comme l'utilisation malveillante du DNS.

De quoi est-ce que je parle ici ? Je parle du fait que depuis le mois de janvier et le mois d'avril 2022 le service conformité de l'ICANN a lancé 230 enquêtes liées à l'utilisation malveillante du DNS, c'est-à-dire que l'ICANN n'est pas passif et n'attend pas passivement à ce qu'il y ait un accord généralisé par rapport à l'utilisation malveillante du DNS. Non, l'ICANN est en train d'agir, d'être actif et de prendre les devants pour atténuer, non seulement atténuer mais lutter activement contre l'utilisation malveillante du DNS.

Comment peut-on lancer une procédure d'action de la part de l'ICANN ? Et bien écoutez, une grande partie de ces actions sont déclenchées par les actions déclenchées par les individus. Ou bien par le biais d'audits qui fournissent les services liés aux noms de domaine.

Donc, à travers tous ces canaux l'ICANN peut envoyer ses notifications à ceux qui sont considérés comme étant en train d'enfreindre certaines dispositions des contrats, notamment la section 3.18. Et, à cet égard, l'action entreprise par l'ICANN a deux étapes : une étape informelle puis une étape formelle.

Le gros des actions est résolu au niveau informel. Pourquoi ? Parce que ceux qui sont notifiés du fait qu'ils sont en train d'enfreindre ou ne sont pas en train de respecter les dispositions du contrat ont la possibilité de réparer cette erreur ou cette action avant de recevoir une notification formelle. C'est pourquoi, j'insiste, le gros des actions se finalise à cette étape informelle. Pour ceux qui décident de ne pas entreprendre d'action pour corriger l'erreur éventuelle par rapport à la non-conformité aux dispositions du contrat, alors on passe à la deuxième étape, celle de l'action formelle où il y a une intervention plus en profondeur de la part de l'organisation. Et si, enfin, cette situation n'est toujours pas corrigée alors on passe à un autre type de mesures.

Mais tout ce que je veux dire avec tout cela c'est que l'ICANN est loin d'être passif et ne reste absolument pas les bras croisés. Au contraire l'iCANN prend toutes les mesures pour atténuer et lutter activement contre l'utilisation malveillante du DNS.

Merci.

HADIA ELMINIAWI : Merci, Léon, pour toutes ces informations. Donc j'ai trois autres mains en attente, mais j'aimerais passer la parole à NARALO, parce que nous avons peu de temps. Donc Eduardo, allez-y.

EDUARDO DIAZ : Je vais également parler en espagnol. Moi je vais vous dire ce que l'on fait au niveau de la RALO pour atténuer et lutter contre l'utilisation malveillante du DNS.

Comment nous, au niveau de la région, nous voyons les choses ? Évidemment, on parle avec les représentants des différentes ALS et on se réunit tous les mois. Et lors de ces réunions mensuelles nous avons organisé des webinaires sur le DNS et plus spécifiquement pour que les gens soient conscients du fait qu'il y a une utilisation malveillante du DNS.

Alors on parle beaucoup de l'abus du DNS, mais très souvent, en marge de l'abus du DNS il y a des choses qui sont liées à la cybersécurité qui n'ont rien à voir avec le DNS, comme les rançons-logiciels. Mais dans mon ALS, à Puerto Rico, on a fait des alliances avec une organisation très connue aux États-Unis, AARP, ce sont des personnes retraitées, de plus de 50 ans, qui travaillent et c'est à eux que s'adressent ces webinaires parce qu'ils ne sont pas conscients du fait que lorsqu'ils reçoivent un mail avec un

hyperlien, ou lorsqu'ils sont sur un nom de domaine, ils peuvent être victimes de délits, d'abus. Et donc on essaye de sensibiliser.

Et on organise également deux événements par an, avec des enseignants de l'enseignement supérieur et on organise avec eux le même webinaire pour les sensibiliser au fait qu'il faut être prudent et attentif à ce genre d'abus.

Et, parfois, on se réunit également avec des professeurs d'université, pour sensibiliser, une fois encore, pour qu'ils soient conscients de ce genre d'abus.

C'est une manière dont on essaye d'atténuer ce phénomène. On essaye de l'atténuer, oui d'accord, mais pour nous c'est difficile d'évaluer l'ampleur de ce phénomène. C'est quelque chose qu'on essaye de faire, mais qui est en cours.

HADIA ELMINIAWI: Merci beaucoup Eduardo, je passe la parole à Graeme qui a une présentation pour nous. Et j'invite Amrita et Claire à mettre leurs questions dans le chat et si nous n'avons pas le temps nous y répondrons directement. Graeme ?

GRAEME BUNTON : Merci. Premièrement nous avons lancé un service qui s'appelle le NetBeacon. Quand je dis nous c'est le DNS Abuse Institute qui est un organisme qui est financé par le BIR qui opère le .ORG.

Cette initiative est soutenue par l'Institut, par PIR et par CleanDNS qui a fait tout ce qui est développement gratuitement donc nous apprécions leur contribution.

Donc NetBeacon a pour objectif de traiter de deux problèmes. Diapositive suivante s'il vous plait.

Nous avons déjà parlé de ceci aujourd'hui donc signaler les abus c'est compliqué, il faut avoir des connaissances techniques, il faut savoir identifier le bureau d'enregistrement, trouver la fonction de signalement d'abus, il faut pouvoir fournir des preuves, il n'y a pas de mise en œuvre cohérente et donc il est difficile pour les utilisateurs finaux de signaler les abus quand ils sont victimes.

Autre problème, les signalements d'abus sont brutaux et c'est difficile de l'apprécier lorsqu'on ne fait pas partie d'un bureau d'enregistrement. Mais les rapports en général n'ont pas de preuve, ils ne sont pas réalisables, ils sont répétitifs, et très souvent on ne peut rien faire. Donc les bureaux d'enregistrement passent énormément de temps et d'énergie à faire le triage de ces rapports et finalement ça ne contribue en rien à la sécurité de l'internet.

Donc nous nous sommes dit qu'on pourrait résoudre ces deux problèmes en même temps et c'était vraiment l'objectif de NetBeacon.

Diapositive suivante.

Donc NetBeacon est un site permettant de signaler les abus de manière gratuite et facile qui améliore la qualité des rapports et qui réduit les obstacles à l'action. L'objectif ici est de faciliter les choses pour que vous puissiez signaler les rapports, donc vous et tous les utilisateurs finaux. Le travail des bureaux d'enregistrement est facilité également et donc il y a des fonctionnalités clefs dans cet outil que nous avons lancé. Il y a une normalisation des exigences et du format, il est facile de signaler, il y a un formulaire qui est assez clair. Il y a aussi enrichissement des rapports, donc nous prenons le nom de domaine soumis, nous prenons les informations qui ont été fournies et nous avons des services de renseignement de noms de domaine que nous utilisons pour améliorer le rapport. L'idée c'est vraiment, du point de vue de la conformité de faciliter les choses.

Et, automatiquement ce rapport est envoyé au bureau d'enregistrement approprié. Donc l'utilisateur n'a jamais à identifier ni même à comprendre ce qu'est un bureau d'enregistrement pour envoyer un rapport.

Diapositive suivante ;

Voilà, vous avez un exemple du formulaire. Là vous avez un problème de hameçonnage, et d'ailleurs je crois que nous avons fait certaines mises à jour depuis cette capture d'écran. Mais c'est relativement clair, les informations sont simples, vous avez des outils qui vous permettent d'expliquer pourquoi, ce qu'on demande, on vous permet de passer par différentes étapes, de sauvegarder le rapport si vous n'avez pas toutes les informations pour continuer plus tard.

Je ris parce que je me rends compte que l'exemple c'est ICANN.ORG, l'exemple d'un domaine hameçonné, désolé, je vais changer ça.

Vous pouvez faire le processus sur le formulaire et envoyer le rapport d'abus. C'est tout et c'est très simple.

Il y a une certaine friction pour certains utilisateurs, il est facile de taper un email, mais malheureusement si vous voulez améliorer tout le processus et bien il faut passer par les formulaires. Et il faut aussi avoir une adresse vérifiée pour utiliser le site. Vous pouvez vous inscrire par un compte Google, vous pouvez créer un compte sur le système mais il faut avoir une adresse email vérifiée. Les plaintes anonymes ne sont pas acceptées parce que c'est trop compliqué pour les bureaux d'enregistrement surtout s'ils ont

besoin de davantage d'information. En plus ceci peut être utilisé à des fins malveillantes si le rapport ne comporte pas d'adresse email vérifiée.

Diapo suivante.

Donc voilà qui a appuyé le travail : l'institut, PIR et Clean DNS. C'est prêt, ça fonctionne depuis le milieu de la semaine passée. Nous avons vu une excellente participation des bureaux même s'ils ne doivent pas nécessairement s'inscrire puisque nous pouvons simplement envoyer les rapports à leur adresse email ; nous avons un certain nombre de personnes qui sont inscrites et qui l'utilisent. Nous avons enrichi certains rapports, envoyé aux bureaux d'enregistrement qui ont agi.

Je suis assez content, cela devrait améliorer les choses et je vous encourage tous à essayer cet outil si vous avez des problèmes d'abus, que vous avez constaté, n'hésitez pas à l'utiliser, partagez ces informations autour de vous, parce que je pense que cela permettra d'atténuer l'utilisation du DNS dans l'écosystème.

Voilà ce dont je voulais vous parler pour l'instant. Je n'ai pas beaucoup de temps donc rapidement je vous parle aussi d'un autre sujet que je souhaitais soulever.

À l'institut, je sais que j'aime bien parler de l'abus, mais ce qui est plus important encore c'est d'atténuer cet abus. Ce que je veux

dire aujourd'hui c'est que vous pouvez faire certaines choses très concrètes pour atténuer les abus.

Donc, lors de la réunion précédente de l'ICANN, il y a eu une plénière assez intéressante à laquelle j'ai participé sur le sujet des sites web détournés par rapport aux enregistrements malveillants et la différence entre les deux. Et la communauté a pu mieux comprendre ce que cela voulait dire et nous avons mieux compris qu'il fallait traiter en fait ces deux préjudices différemment. Il y a encore du travail à faire dans ce domaine et vous verrez que les parties contractantes publieront des informations avant la prochaine réunion de l'ICANN, si tout va bien.

Mais il y a quand même quelque chose intéressant ici et qui est important pour les utilisateurs finaux, si vous regardez la nouvelle étude sur l'utilisation malveillante du DNS, vous pouvez voir que 25 à 41 % des rapports ou des signalements d'abus ce sont en fait des sites détournés, ce n'est pas des enregistrements malveillants. Donc cela veut dire que quelqu'un utilisait un site web qui a été piraté et qui maintenant est utilisé à des fins malveillantes. C'est donc 25 % pour le hameçonnage et 41 % pour les programmes malveillants, mais ça dépend et il peut y avoir des variations dans ces pourcentages.

Donc c'est quand même important, 41 % des programmes malveillants sont liés à des sites qui sont détournés. Et il faut faire

quelque chose. Et nous le pouvons. Et je crois qu'à l'ALAC c'est un domaine où vous pouvez influer.

Alors il y a des choses très simples finalement : avoir une hygiène de mots de passe qui soit saine, donc des mots de passe qui soient difficiles à deviner, de manière à ce que les choses ne soient pas piratées, activer l'identification à deux facteurs sur votre site web, autant que possible. Si vous avez un site web, si vous avez une petite entreprise, quel que soit le cas, activez les mises à jour automatique sur votre CMS et les plug-ins également, cela fait partie d'une exploitation saine et responsable des sites web. Donc acquérir des thèmes et plug-ins de sources de bonne réputation. Parfois on a des thèmes intéressants mais qui comportent des programmes malveillants. Donc faites attention à l'acquisition de vos sources.

Et, ensuite, vous pouvez tous partager ces meilleures pratiques et au DNS Abuse Institute nous avons un blog assez long qui a été publié, que je vais mettre dans le chat, qui couvre beaucoup de ces questions dans les détails. Mais il faut donc traduire, partager à tous. Et donc pour terminer NetBeacon n'est qu'en anglais. Donc nous essayons de voir un petit peu ce que nous pouvons faire pour améliorer le système, cela ne fait qu'une semaine qu'il a été lancé et nous avons du travail au niveau de l'internationalisation et

j'espère qu'au cours des mois à venir nous pourrons avoir une interface dans les langues des Nations Unies, au moins au départ.

Donc voilà deux points vraiment très concrets sur lesquels cette communauté pourrait se concentrer pour réduire ou atténuer l'utilisation malveillante du DNS.

Merci.

HADIA ELMINIAWI: Merci beaucoup, Graeme, c'est très intéressant de connaitre ce site de signalement d'utilisation malveillante du DNS qui est gratuit, NetBeacon, et de savoir comment mieux se protéger contre les sites détournés.

Donc je crois que nous sommes en fait en retard. Donc merci beaucoup d'avoir participé à cette séance, toutes nos excuses, nous n'avons pas pu écouter toutes les questions et nous n'avons pas pu lire tous les commentaires dans le chat, mais nous espérons pouvoir y revenir lors d'une autre séance de l'At-Large. Merci à tous, la séance est levée, l'enregistrement est terminé.

[FIN DE LA TRANSCRIPTION]