FR

ICANN83 | Forum de politiques – Séance plénière d'At-Large 2 : Progression des efforts de l'atténuation de l'utilisation malveillante du DNS au sein de l'ICANN
Jeudi 12 juin 2025 – 10h45 à 12h15 CEST

BRENDA BREWER

Bonjour et bienvenue à cette réunion plénière At-Large concernant l'atténuation de l'utilisation malveillante du DNS. Je serai le gestionnaire de la participation à distance pour cette séance, avec mes collègues. Cette session est enregistrée et régie par les normes de comportement attendues de l'ICANN ainsi que les règles anti-harcèlement de la communauté de l'ICANN.

Lors de cette séance, les questions et commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre questions et réponses. L'interprétation sera assurée en anglais, français et espagnol.

Si vous souhaitez prendre la parole, veuillez lever la main dans Zoom, lorsque vous serez appelé, les participants à distance auront le droit d'activer leur micro. Les participants sur place utiliseront un micro physique pour parler. Veuillez donner votre nom pour l'enregistrement et la langue dans laquelle vous allez vous exprimer si ce n'est pas l'anglais. Et veuillez parler à un rythme raisonnable pour permettre aux interprètes de travailler. Je passe la parole à Jonathan Zuck, président de l'ALAC.

JONATHAN ZUCK

Merci, merci de vous joindre à nous dans le cadre de cette réunion intercommunautaire. Nous allons faire un peu de débats sur ces problématiques. C'est une conversation que nous avons depuis longtemps et on en parle pratiquement à chaque fois dans toutes les réunions. Et Justine me le disait, on est au milieu du chemin, dirons-nous. Je sais qu'il y a une certaine frustration parfois au sujet de l'utilisation malveillante du DNS, le CA n'est pas toujours satisfait de ces points, il y a différentes perspectives, il y a différents fardeaux également qui existent par rapport à ces thématiques.

Donc comme Brenda nous l'a dit, nous avons besoin de règles de comportement, garder notre calme et travailler en coopération.

Voilà, nous allons vous demander de faire quelques suggestions, donc de ne pas nous donner une liste sans fin, il faut que l'on soit en mesure de pouvoir y répondre. En ce qui concerne l'ordre du jour et At-Large, nous n'avons pas une expertise précise dans ce domaine, nous ne faisons pas de rapport sur les abus de l'utilisation malveillante du DNS, nous voulons voir ce qu'il est possible d'effectuer pour limiter cela et essayer de bien comprendre le problème.

Mais ici, dans la communauté de l'ICANN, nous voulons continuer à parler de cela et éviter qu'il y ait une utilisation malveillante du DNS qui se poursuit et s'amplifie. Donc, ce que nous avons à l'esprit et qui pourrait être notre domaine de priorité, c'est une exploration des corrélations associée avec les enregistrements en vrac. Je ne sais pas s'il y a une définition standard de cela. Il y a eu des

recherches qui ont été faites sur ces enregistrements groupés. Et il y a un grand nombre d'enregistrements qui sont effectués en même temps, ça a été compliqué par l'IA où beaucoup d'enregistrements peuvent être effectués au même moment, tout cela pour des abus et des utilisations malveillantes.

Deuxièmement, nous avons le concept du pivot. Ça, c'est une idée qui existe depuis pas mal de temps, essayer de comprendre, quand un domaine est identifié et qu'il est associé avec un titulaire de nom de domaine, comment retirer ce domaine et déterminer si ce domaine est problématique et doit être retiré.

Voilà les choses qui nous intéressent. Je vais passer le micro à Mason Cole.

MASON COLE Bonjour à toutes et à tous, je suis pendant deux semaines encore à la tête du CSG. Et je crois que j'avais une présentation.

JONATHAN ZUCK Y a-t-il une présentation pour Mason ? Du groupe des parties prenantes commerciales ?

MASON COLE Oui, le CSG, je suis aussi président du BC, des entités commerciales, on a été très actifs sur l'utilisation malveillante du DNS. À Istanbul nous avons travaillé au CSG pour essayer de trouver de nouveaux

outils pour combattre l'utilisation malveillante du DNS. Et je suis très heureux de voir que cela se chevauche dans la communauté.

Il y a beaucoup de points qui se chevauchent entre ce que propose le CSG et d'autres parties de la communauté. C'est bien de savoir qu'il y a des outils qui peuvent être utilisés pour faire quelque chose et réagir.

Une mise en contexte, d'abord. Ce n'est pas nouveau, l'utilisation malveillante du DNS est une question qui se pose depuis longtemps, ça ne va pas être résolu du jour au lendemain pour la prochaine série. Il va y avoir des outils d'identification, il va toujours y avoir de l'utilisation malveillante du DNS et c'est un problème endémique, dirons-nous, qui existe à l'interne et qui pourrait être éradiqué. Nous avons vu, depuis le début de l'internet, on peut citer les premiers pourriels reçus dans les années 79, donc cela fait 45 ans. Le problème est mondial, il s'étend, s'intensifie et cela représente des chiffres énormes. L'économie de la cybercriminalité c'est 9,5 trillions de dollars. Cela provient du forum économique mondial, ce serait la troisième économique du monde, c'est énorme.

Donc nous savons de l'utilisation malveillante du DNS doit être absolument définit et résolut. Parce que nous avons des entités commerciales qui ont à souffrir d'un impact commercial et financier lors de l'utilisation malveillante du DNS. Et il faut donc le définir et le résoudre. SSAC 115 avait donné des opinions, ils nous ont indiqué que pour la définition de l'utilisation malveillante du

DNS, et c'est dans les contrats de l'ICANN, ça ne couvre pas tous les types de l'utilisation malveillante du DNS qui sont reportés par les prestataires de services, de nouveaux types d'abus sont créés et qui vont et viennent avec le temps. Donc il n'y a pas une liste précise du type d'abus qui sera toujours complète. C'est très difficile à définir, lister et préciser.

Diapo suivante. La suivante dans la série de la présentation

On m'a demandé quelques thématiques qui nous intéressent particulièrement, de donner le raisonnement derrière cela et des questions de politiques potentielles. Donc lorsque nous avons un développement de ces utilisations malveillantes et de ces abus sur plusieurs domaines, avec un seul titulaire de nom de domaine ou des comptes d'un bureau d'enregistrements multiples avec un seul titulaire de nom de domaine, c'est un nouveau problème et c'est quelque chose qui peut être attaqué et précisément sur un compte ; il y a un nom de domaine, avec un seul titulaire, mais il n'y a pas de visibilité à l'extérieur pour véritablement savoir à quel point cet acteur néfaste abuse de la situation. Donc on a besoin d'un aide au niveau du bureau d'enregistrement pour une atténuation de la situation. Parce que le travail uniquement au niveau du nom de domaine n'est pas efficace.

Quel type de politique ? Comment codifier une atténuation au niveau du compte, du contrat, des meilleures pratiques et comment documenter la résolution et redonner ce document de résolution. Parfois, on travaille avec les bureaux d'enregistrement

et il y a des actions prises ou non, mais on ne sait pas toujours ce qui a été fait par la personne qui a rapporté l'abus.

Donc les imposteurs, on l'a vu en octobre dernier, dans les médias, on a entendu parler de cela aux États-Unis, un sénateur américain a envoyé une lettre pour parler de ce problème des noms de domaine. Par exemple FOX-NEWS.TOP, Fox News est une chaine d'informations aux États-Unis et le sénateur était inquiet, il pensait qu'il y allait avoir des noms de domaine enregistrés et qui allaient faussement envoyer des personnes vers de fausses informations et on n'était pas loin des élections américaines. Ça, c'est du squattage, quand les noms ne sont pas exactement les mêmes, avec des marques déposées qui sont détournées un peu, avec des erreurs typographiques, des lettres supplémentaires ou quoi que ce soit.

L'UDRP n'est pas très efficace parce qu'il n'est pas assez rapide ;, ce processus de résolution des conflits. C'est un processus trop lent qui ne peut pas être développé non plus, et ce n'est pas sur assez de noms de domaine. Donc la question de politique c'est comment créer un mécanisme pour que les bureaux d'enregistrement puissent être utiles et comment définir un standard, une norme pour agir contre ce type de problèmes où on prend une marque et on la détourne par exemple.

Donc il faut bien comprendre ces situations et cela va être important de définir un standard à long terme pour gérer ces imposteurs, ces noms de domaine qui sont des imposteurs.

Je crois que j'ai peut-être terminé.

JONATHAN ZUCK

Vous avez terminé, de toute façon c'était très utile. Merci à vous. Maintenant nous allons passer la parole à Gabriel.

GABRIEL ANDREWS

Bonjour, je suis co-président du groupe de travail sur la sécurité publique. Je suis aussi impliqué dans une organisation des forces de l'ordre aux États-Unis, le FBI. On va parler de la perspective des forces de l'ordre, on n'a pas toujours la même perspective que les autres dans la salle.

Pour vous donner une idée, sachez que quand les gens viennent nous voir, ils sont victimes d'un crime, nous avons un portail à travers lequel ils peuvent déposer leur plainte, c'est IC3.GOV. Cela nous aide à compiler les informations de tous les mauvais acteurs qui victimisent la population. Cela nous permet aussi d'ouvrir les investigations et de connecter les statistiques de différents types de crimes. Même si c'est centré aux États-Unis, on a quand même des rapports qui viennent de partout et on voit que les catégories les plus importantes sont assez similaires à travers le monde.

Les perspectives que l'on voit sont liées aux questions politiques potentielles. On voit les crimes qui sont rapportés par rapport au montant de pertes en dollar. Il y a la fraude des investissements en crypto. Et si vous ne connaissiez pas cela, vous devriez étudier cette question et prendre le temps d'aller sur You Tube et voir ce qu'a fait

Johan Oliver, la semaine dernière il a fait une émission là-dessus, c'est très important de connaitre ces données pour se protéger et protéger sa famille ; ce sont des gens qui essayent de convaincre les gens d'investir en cryptomonnaie. On a vu que ces gens sont souvent impliqués dans des enregistrements groupés, cela arrive très souvent, pour créer des échanges de fausse cryptomonnaie.

Comment les politiques peuvent introduire la friction justement dans l'utilisation malveillante de ces outils qui font des enregistrements regroupés C'est vraiment la catégorie la plus importante de crimes qui nous sont signalés.

Deuxième question : imaginez le nombre de plaintes que l'on reçoit, on n'organise pas ça par perte en dollars, mais ce qui nous est signalé le plus souvent ; en général c'est le hameçonnage, mon ami Brian Cimbolic me disait hier : si on avait la capacité de séparer tout ce qui était fishing dans les courriels, tout ce qui était basé le hameçonnage, mais ce n'est pas possible ; on sait très bien que les domaines qui font du hameçonnage sont enregistrés d'une manière malveillante, ce sont des homoglyphes.

Il y a aussi des enregistrements qui sont répétés, qui sont des domaines qui usurpent de vrais domaines et qui usurpent aussi de vraies victimes.

JONATHAN ZUCK

Merci, Gabriel, et merci à vous deux d'avoir démarré la conversation. Maintenant, peut-être qu'on a des réactions au sein

de notre groupe et que nous pouvons apporter différentes perspectives, des opérateurs de registres ou même des réactions liées aux droits humains. Dennis ?

DENNIS TAN

Bonjour, je travaille pour Verisign, mais je représente le groupe de travail des registres, j'ai été aussi président avec mon collègue Reg de ce groupe de travail sur l'utilisation malveillante du DNS. Sachez qu'ul y a des points communs.

Je vais prendre un peu de recul, lundi la CBH et le comité de sensibilisation sur l'utilisation malveillante du DNS ont présenté 4 thématiques de travail potentiel à la considération de la communauté. Voilà les sujets : l'idée pivot ou ce qu'on appelle aussi la vérification des domaines associés, deux : le renforcement des obligations des enregistrements des revendeurs en termes de l'utilisation de l'interface de programmation d'application et toutes les exigences liées à l'atténuation de l'utilisation malveillante du DNS. Ensuite on a parlé des botnets, réseaux zombie, et on a parlé aussi de l'information qui devrait être partagée avec la DGA, donc les algorithmes de génération de domaine, des réseaux zombie utilisent des centaines et des milliers de listes de noms de domaine qu'ils peuvent enregistrer par lot, ils utilisent cela pour faire des attaques de hameçonnage. Donc on essaye de proposer des systèmes qui pourraient nous permettre de faire du travail technique de manière précoce pour éviter que les DGA se produisent.

Donc, on essaye de savoir comment on pourrait signaler le hameçonnage et à qui. Il y a les rapports qui manquent d'éléments probants par exemple ou mal signalisés. Comment peut-on, avec la communauté ICANN, augmenter la qualité de ces normes pour pouvoir arriver à signaler les abus de manière bonne.

Voilà un peu, c'est sur cela que nous travaillons et je pense que l'ALAC a proposé deux idées. C'est la corrélation de l'utilisation des enregistrements groupés avec l'étude d'Infermail. Comme vous le voyez à l'écran. Et, encore une fois, on revient sur cette idée de pivot dont vous avez parlé. Ce sont les deux choses dont vous avez parlé qui chevauchent les idées de la CPG. Nous travaillons à des idées similaires à la CSG. En premier nous parlons des enregistrements groupés malveillants.

Non, attendez, je me suis trompé. Désolé, je n'ai pas mes lunettes et je ne sais pas où j'en suis, j'essaye d'ajuster.

Alors, on parlait des domaines imposteurs. On va continuer la conversation dans ce sens avec les deux idées que vous avez développées vous-même. Au PSWG quelqu'un a parlé de la friction des enregistrements groupés en utilisant API, ces outils chevauchent aussi ceux qui sont utilisés par la CPH.

Je voudrais clarifier quelque chose. Il faut essayer de comprendre ce que vous dites quand vous parlez d'enregistrements malveillants répétés et qualifiés. Quand vous parlez de hameçonnage aussi. Alors, les noms de domaine de hameçonnage pour des buts et objectifs malveillants, est-ce que vous avez noté

que les politiques de procédure qu'on a aujourd'hui ont des carences ?

GABRIEL ANDREWS

Tout d'abord, les acteurs malveillants vont peut-être enregistrer un certain nombre de noms de domaine, sous un nom avec un paiement, essayer d'échanger de nom et le faire et refaire. Mais j'espère qu'en discutant on peut essayer de voir comment on peut détecter ces activités. Avez-vous une idée un peu du niveau d'action qui peut être entrepris ? Peut-être qu'il y a l'idée d'avoir plusieurs comptes. Comment faire un suivi de cela ? L'idée pour eux est de revenir vers la source et d'empoisonner la source encore et encore. Comment peut-on faire une fois au lieu de retourner en arrière pour trouver des choses probantes à chaque fois qu'ils font un nouvel enregistrement ?

DENNIS TAN

On ne parle pas de noms de domaines enregistrés par lot, ils font cela en changeant une lettre. Ils viennent, ils essayent, changent un peu, modifient le nom et reviennent encore en utilisant un même modèle et testent pour voir si cela passe et ils enregistrent un nouveau compte. Ils utilisent d'autres identifiants, etc.

GABRIEL ANDREWS

Comme l'a dit la CPH, la méthode est celle du pivot, il y a peut-être un peu de chevauchement avec ce que vous faites. Mais il faut qu'on arrive à mettre en œuvre des politiques qui soutiennent des

actions et des choses qu'on peut faire quand il s'agit de contrecarrer ces comportements.

JONATHAN ZUCK Reg, vous souhaitez prendre la parole ?

REG LEVY Je fais partie du groupe des parties prenantes des bureaux d'enregistrement, je travaille avec des groupes de travail sur l'utilisation malveillante du DNS. Donc c'est intéressant, tout cela est intéressant et on est très heureux qu'il y ait des propositions qui nous ont été présentées. Nous allons rapporter cela à toutes les parties prenantes intéressées. Comme Dennis l'a dit, il y a souvent du chevauchement, je pense que nous allons continuer à en discuter et à travailler et à collaborer.

JONATHAN ZUCK Merci. Graeme ?

GRAEME BUNTON Bonjour à tous. Je suis directeur exécutif de l'institut NeBeacon et nous sommes une partie importante du registre sur l'intérêt public et nous nous focalisons beaucoup sur le travail fait en ce qui concerne l'utilisation malveillante du DNS. Nous avons publié un livre blanc, il y a deux semaines, et nous avons fait cela pour un couple de raisons. Tout d'abord, c'est un enjeu sur lequel nous discutons depuis longtemps, nous avons pensé qu'il fallait pousser

un peu plus pour voir ce que l'on peut faire, surtout lorsqu'il s'agit des amendements contractuels de l'année dernière pour les opérateurs de registre et bureaux d'enregistrement.

Nous voulions essayer de modeler cette nouvelle conversation parce que nous pensions qu'il y avait encore des carences. Donc nous avons émis quelques idées et publié ce papier blanc. Ce papier a été une approche, nous voulons continuer à avancer des idées à la communauté en même temps que nous avançons dans nos travaux.

Diapo suivante.

Je vous ai parlé de NetBeacon, nous voulons tous travailler dans le modèle multipartite, connaitre le succès dans la communauté de l'ICANN. Nous pouvons avancer et régler des problèmes importants. Comment effectuer quelque chose, obtenir un résultat, comment fournir des exemples à une envergure étroite, à quoi cela va-t-il ressembler ? Comment envisager l'envergure du problème et des solutions que nous allons pouvoir proposer ?

Diapo suivante.

Je ne vais pas rentrer dans les détails ici parce que je crois qu'on a déjà couvert beaucoup dans diverses présentations, on a parlé du pivot, des enregistrements malveillants et comment lutter contre cela. Mais ce que j'aimerais souligner ici c'est quelle est la différence entre un processus réactif et proactif pour réduire les abus. Vérifier le compte des clients, cela prend du temps et c'est un

travail qui peut être intéressant néanmoins. Ce que l'on pense à l'institut, c'est qu'avec le conseil de notre NetBeacon cela représente des financements nécessaires, des frais. Est-ce qu'on doit donner l'accès à ces différents outils quand on a des enregistrements par volume ? Donc la communauté doit réfléchir à cela, comment réagir largement à ces utilisations malveillantes et comment éviter cette utilisation malveillante avec un effet d'échelles.

En ce qui concerne les interfaces d'informations de programmation et d'application et des portails, quand nous avons des domaines nuisibles enregistrés en masse, que peut-on trouver pour limiter l'utilisation et avoir des outils qui permettent de ne pas bloquer les titulaires de noms de domaine tout à fait légitimes.

Donc nous pensons que cette friction doit être basée sur la réputation du client, pas sur qui est le client, mais quelles activités ont-ils déjà effectuées. Je pense que cela intéresse beaucoup, cette vérification des titulaires de domaine, de même que l'exactitude des données. Mais c'est miné comme terrain, aussi, parce que nous devons travailler rapidement et de manière efficace. Et, également, dans certaines circonstances, il faut être très prudent par rapport au vol d'identité.

Donc, lorsqu'on réfléchissait à cela, comment cela peut fonctionner, je crois qu'il est important pour être productif de se baser sur les activités des titulaires de noms de domaine, combien de domaines ont-ils sur une plateforme, ont-ils renouvelé leur

domaine, quelle est la réputation et leur historique. Mais cela peut être totalement erroné parce qu'il est difficile d'effectuer une vérification d'identité parce qu'il y a ces lois de respect de la confidentialité et on se retrouve coincé. Donc est-ce que c'est la bonne approche ? Est-ce que cela va être efficace ? Est-ce que cela va permettre d'éviter la fraude ?

Donc on voit de l'utilisation malveillante du DNS au niveau du sous-domaine, c'est pour que les bureaux d'enregistrement aient un outil pour pouvoir parler aux titulaires de nom de domaine et leur offrir des domaines avec des parties tierces et faire passer ces obligations des bureaux d'enregistrement aux titulaires de nom de domaine.

IL n'y a pas de mécanisme de respect, mais c'est un outil pour les bureaux d'enregistrement pour influencer des services responsables. On n'a pas beaucoup, au troisième niveau dans les gTLD, parce qu'il y a de grandes conséquences ; mais nous avons ici un outil pour les bureaux d'enregistrement pour approcher les services qui génèrent beaucoup d'abus au niveau des sous-domaines et pouvoir indiquer aux bureaux d'enregistrement que votre domaine connait un risque.

Prochaine diapo.

Nous avons des mécanismes de recours pour les titulaires de noms de domaine, les personnes impactées qui ont eu leur domaine

suspendu. Il faut un accès transparent et raisonnable et qu'il y ait des recours possibles ;

En ce qui concerne les réseaux zombie, botnet et la coordination des GA, nous devons véritablement travailler avec les registres indépendamment pour gérer ces réseaux zombie et pour avoir des fonctions plus efficaces. Cela n'a pas à être un PDP, il y a d'autres manières de travailler là-dessus.

Je voulais noter cela ici, je crois que c'est une petite fréquence, mais un impact fort, cela n'arrive pas souvent, mais quand cela arrive c'est dommageable.

Alors les résultats, le résumé des résultats de notre institut de NetBeacon, c'est que nous voulons tous avancer et faire des progrès et nous avons besoin de définir l'envergure du travail que nous allons faire et nous devons faire des progrès, très clairement. Tout le monde ne devrait pas avoir ce qu'il désire obtenir ; nous devons nous concentrer sur des points plus étroitement pour connaitre des progrès. Et je crois qu'on pourra faire pas à pas des progrès. Et je crois qu'au niveau des thématiques il y a eu des amendements mis en place et des obligations claires pour des rapports individuels sur les abus. Ça, c'est très bien pour l'écosystème.

Néanmoins, c'est clair également pour nous, quand on voit les données, le service Map par exemple ou les rapports NetBeacon, nous voyons que les abus sont de grandes campagnes d'utilisations malveillantes, donc comment gérer cela en tant que

communauté, d'une manière sûre et responsable. C'est la grande question. Merci.

JONATHAN ZUCK Merci, Graeme, vous avez indiqué des points importants en termes de remédiation, c'est intéressant. Farzaneh ?

FARZANEH BADIEI Merci de l'invitation, je suis membre des entités non commerciales, et le NCSG s'intéresse beaucoup à la liberté de parole et d'expression, accès aux connaissances. Et en tant qu'utilisateurs finaux, l'accès aux connaissances est très important, c'est une question de droits humains.

J'aimerais être très clair, nous voulons atténuer l'utilisation malveillante du DNS, c'est nécessaire et doit être fait. Néanmoins, nous ne sommes pas d'accord avec l'aspect urgent dont vous parlez. Vous dites l'urgence, tout le temps. Et on a des statistiques qui ne sont pas seulement les crimes qui sont le résultat direct de l'utilisation malveillante du DNS. Cela peut être pour d'autres problèmes et provenir d'autres problèmes et sources. Mais l'atténuation est très importante parce qu'en tant qu'activistes et défenseurs des droits humains il peut y avoir un impact néfaste avec de l'hameçonnage et des acteurs étatiques qui peuvent faire cela. Donc on doit atténuer, cela peut améliorer les droits humains.

Donc, mettre des statistiques et dire que l'internet est en train de mourir et qu'on est en plein abus et utilisation malveillante, ce

n'est pas exact et on va prendre des décisions trop rapides et hâtives. J'apprécie les recommandations apportées, mais je pense que nous devons rester dans le cadre de l'ICANN et de la mission de l'ICANN et il faut prendre en compte les risques par rapport aux droits humains.

Comment allons-nous avoir un impact sur les titulaires de nom de domaine et d'utilisateurs finaux de l'internet quand on atténue l'utilisation malveillante du DNS. La société civile a des outils pour l'évaluation sur les droits humains et cela ne doit pas se passer par la suite, mais cela doit se passer tandis que nous faisons notre atténuation de l'utilisation malveillante du DNS. J'ai un collègue qui dit, quand on parle de l'accès et des remèdes, est-ce que cela va être avant qu'il soit mort ou après qu'il soit mort ? C'est une plaisanterie de personnel médical. J'exagère un peu, mais ce que nous devons faire, comme l'a dit Graeme, c'est trouver des solutions. Mais cela ne doit pas être l'identification des titulaires de nom de domaine, c'est très important pour le NCSG de protéger les droits humains que les titulaires de nom de domaine puissent rester anonymes. C'est essentiel pour les utilisateurs de l'internet et pour les noms de domaine et pour les bureaux d'enregistrement. La confidentialité et le respect de la vie privée comptent beaucoup, la liberté d'expression aussi. Quand nous suspendons un nom de domaine néfaste ou usurpé, compromis, on peut suspendre l'accès à des informations, à des savoirs, à des campagnes qui se déroulent.

Donc, également, Mason a mentionné les imposteurs, les domaines imposteurs ne sont pas une utilisation malveillante, c'est une question de contenu. Au NCSG on ne gère pas cela, on veut rester technique dans la définition de l'utilisation malveillante du DNS tel qu'elle est dans le contrat régi par l'ICANN. Nous avons un exemple donné, ce n'est pas de l'utilisation malveillante du DNS et l'ICANN n'a pas de rôle à jouer dans la lutte contre les fake news, c'est au niveau mondial que cela se déroule, au niveau des régulations et règlements juridiques mondiaux.

J'ai quelques recommandations, je serai brève. J'aimerais remercier Graeme pour tout son travail et ses efforts. Nous devons voir vos recommandations de près, les analyser et débattre de la manière dont cela peut avoir un aspect positif sur l'évaluation des droits humains, comment on peut prendre ces recommandations, les mettre en œuvre sans impacter d'une manière négative les droits humains par exemple. Rapidement, si on fait une étude, cela peut avoir un impact quand il y a un groupe de noms de domaine. Je ne veux pas en dire plus, car nous devons analyser les recommandations faites.

JONATHAN ZUCK

Merci de votre point de vue, on essaye de trouver un équilibre ici et d'accomplir le plus dans ce qui est nécessaire avec des conséquences positives. Donc je crois que tout le monde a pris la parole au niveau du panel, quelqu'un veut répondre à quelque chose qui a été déjà dit ? Oui ?

GABRIEL ANDREWS

J'ai pris quelques notes, Graeme, quand vous parliez, si j'ai bien compris, votre point 5 était impliqué dans les contemplations de l'ICANN quand il s'agit du rôle pour l'implication des botnets DGA. C'est quelque chose que nous devons continuer d'explorer avec vous, avec les parties contractantes. À ce moment-là, cela pourrait nous être utile.

S'agissant du point 2, pour entrer des frictions avec API pour des enregistrements, malicieux, je parle en ma propre capacité, pas pour le PSWG, je réagis quand je vois ce rapport INFERMAL avec 400 % d'augmentation au niveau des abus. Donc je pense qu'il est important pour moi de prendre du recul et de reconnaitre que la chose clef ici est la prévention.

Il s'agit, au bout du compte, peu importe si on utilise la voie 1, 2 ou 3, il faut faire de la prévention. Comment on peut mettre en œuvre des idées qui vont nous permettre de mesurer ? Et comment allons-nous mesurer ce qui va être fonctionnel ? Je serais très heureux de collaborer avec vous et merci de nous rapporter toutes ces idées et j'espère que nous allons pouvoir collaborer, car nous avons les mêmes intérêts.

EUNICE ALEJANDRA PEREZ COELLO

Bonjour, je vais prendre la parole en espagnol. J'ai un doute quand il s'agit de choses qui ont été présentées. Si, de plus, on prend en compte les enregistrements ou les groupes qui enregistrent et qui

offrent des noms de domaine pour des IP dynamiques. S'il y a du suivi qui est fait et je connais - en particulier des services – quelqu'un qui offre des noms de domaine en ligne et en fait c'est facile, on crée son nom de domaine et on peut ensuite utiliser différents dispositifs qui sont faciles à utiliser, encore une fois.

Donc si on fait ce contrôle par rapport à ces enregistrements, s'ils sont considérés comme des enregistrements, si on prend en compte de plus que comme utilisateur final on n'a pas les connaissances nécessaires pour pouvoir mettre en œuvre des mesures de sécurité, parce que là on devient très vulnérable.

JONATHAN ZUCK Qui veut répondre à cette inquiétude ? Graeme ?

GRAEME BINTON Je parlais de cela, on en a parlé dans notre papier blanc. Derrière ce travail potentiel, il fallait faire face à des services qui offraient des services spécifiquement pour le sous-domaine ; mais cette partie qui correspond au DNS dynamique, c'est différent ; si seulement j'avais un meilleur exemple à présenter à la communauté. D'ailleurs, Bryan, vous participez ici, dites quelque chose si vous pensez que je me trompe. Je pense qu'il y a 40 % des utilisations de .ORG qui venaient d'un simple fournisseur de service de sous-domaine, donc un nom de domaine unique sur 11 et quelques millions responsable de 40 % des utilisations

malveillantes des URL. Donc ce n'est pas très commun ce problème au niveau des TLD quand il y a des sous-domaines.

Donc, comment faire pour garantir une certaine responsabilité ? Il y a eu une tentative de le faire d'ailleurs, si Makele était là il pourrait vous en parler. Mais le sentiment était : si vous gérez un service ou un internet utilisé par des parties tierces, c'est inévitable que ce service soit usurpé ou utilisé de mauvaise manière. Il y a des exigences de base quand on offre un service, que les tierces parties doivent être utilisées, il faut maintenir un contrat. Les gens vont abuser des choses quand elles sont disponibles, de toute façon. Donc il faut absolument faire une tentative et fournir une responsabilité. Il faut que ces obligations soient raisonnables aussi.

Quand on utilise ces services, sur votre propre réseau vous avez peut-être exposé tous vos dispositifs d'internet des objets aussi en même temps. Il faut faire des patchs, il n'y en a pas encore pour toutes ces vulnérabilités.

EUNICE ALEJANDRA PEREZ COELLO J'ai une autre question, je vais encore parler en espagnol.

ALAN WOODS J'étais au répertoire de registre et maintenant je suis à CleanDNS. J'ai écouté ces conversations et c'est toujours bon d'avoir le point de vue de quelqu'un qui est au milieu, entre les opérateurs de registre et les groupes externes. Il faut mesurer ce qu'il se produit.

Par exemple, quand il s'agit des amendements, s'il faut pouvoir nous lier aux l'utilisation malveillante du DNS. Il faut utiliser les leçons apprises. Quand on regarde les problèmes, on étudie des statistiques, on a vu des statistiques cette semaine qui ont montré l'échelle et l'ampleur du problème. Et quand on parle de statistiques qui montrent l'ampleur du problème, on a tendance à passer à des conclusions et on pense à l'effort des bureaux d'enregistrement, des opérateurs de registre et on se focalise dessus.

L'autre jour, il y avait une liste de bureaux d'enregistrement qui utilisaient des enregistrements groupés. Donc, par définition, les bureaux d'enregistrement et leurs enregistrements sont atténués. Dans cet exemple il y avait 7 000 enregistrements groupés utilisés, c'était compliqué. Donc il faut faire très attention parce que quand on retire aussi des noms de domaine on pose des problèmes aux agissements des forces de l'ordre. Et là, parfois, il nous faut agir pour les bureaux d'enregistrement et les opérateurs de registre, il n'est pas facile de trouver les actions appropriées et il faut le faire avec les parties appropriées et au moment approprié. Lorsqu'il y a des éléments probants. Je ne vais pas citer de nom, mais une réunion a été faite il y a 6 mois, il y avait 220 000 signalements arrivés pour trois clients précisément, il y avait même 1 % de ces plaintes qui avaient des éléments probants.

Alors qu'on étudie les prochaines étapes pour faire face à ces problèmes. Il nous faut nous focaliser et ne pas tirer les forces de l'alarme de suite, il faut mesurer les actions appropriées par les

bureaux d'enregistrement et les opérateurs de registre. Et il y a d'ailleurs un opérateur de registre qui a fait les grandes lignes il n'y a pas très longtemps pour tout ce qui est des amendements liés à l'utilisation malveillante du DNS. Donc on doit mettre en place des vérifications de tous les rapports qui nous sont envoyés et il faut faire très attention avant de mettre les gens sur des listes de blocage. Il faut être patient et faire attention aux approches que l'on va mettre en œuvre, il ne s'agit pas de mettre tout sur les épaules des bureaux d'enregistrement et des opérateurs de registre, il s'agit de collaborer au sein de l'écosystème en général.

JONATHAN ZUCK C'est bien de parler de l'abus du DNS en disant qu'on doit être calme et ne pas s'énerver.

FARZANEH BADIEI L'existence des liens de hameçonnage ne veut pas dire que les dommages ont déjà été faits. Il y a quelque chose qui manque dans cette conversation. Le nombre de signalements de liens de hameçonnage. Bien sûr, cela porte un risque important, mais les termes utilisés sont importants, si le dommage n'a pas encore été fait parce que le lien n'a pas été utilisé par l'utilisateur final, cela change la donne. Donc, quand on tire la sonnette d'alarme sur quelque chose, trop vite, les solutions de réponse peuvent être assez agressives. Il faut faire attention, car on doit continuer à respecter les droits humains.

JONATHAN ZUCK D'un autre côté, et d'ailleurs peut-être que Gabriel nous l'explique un peu plus, nous savons qu'il y a beaucoup de dommages qui sont faits et beaucoup d'argent impliqué. Il y a quelque chose qui doit nous alarmer dans tout cela. Mais on ne devrait pas forcément réagir trop rapidement ou violemment ; mais je pense qu'il ne faut pas oublier qu'il y a de grands dommages qui sont faits et actés. Michele ?

MICHELE NEYLON Je voudrais faire écho à ce qu'on dit Farzi et Alan. Ceux qui s'impliquent à l'ICANN ici, nous voulons un internet sûr, stable et utile et nous voulons qu'il y ait un certain équilibre à travers l'écosystème. Mais nous savons qu'il y aura aussi de mauvais acteurs. Donc le problème que nous avons ces dernières années est que la concentration a été sur le fait qu'il fallait faire la chasse à l'utilisation malveillante du DNS. Et le seul outil que nous avons est un marteau et donc on a besoin de changer notre mentalité sur l'approche. Oui, bien sûr, beaucoup de mauvaises choses se produisent, de la fraude, cela impacte tout le monde, ma famille, mes clients, mes amis et mes ennemis. Mais il nous faut essayer d'améliorer l'expérience en général au lieu de constamment de chercher tout ce qui est lié à l'utilisation malveillante. Si on continue à rechercher les abus, tout devient négatif, obscur. Donc il nous faut tout de même continuer à essayer à avoir une bonne expérience.

C’est un peu pour cela qu’on voudrait utiliser cette idée de pivot aussi, les utilisateurs finaux passent d’utiliser des domaines aux plateformes et aux applications et perdent le contrôle. Il n’y a pas moyen de faire du suivi. C’est terminé et c’est fait. C’est certainement ce que nous voulons, nous, parce que beaucoup d’entre nous a fait beaucoup de choses et on a vu aussi que beaucoup de choses sont faites à cause de l’internet, des petites et moyennes entreprises existent aujourd’hui grâce à l’internet, de nombreuses choses ont changé ces 10 dernières années.

JONATHAN ZUCK

Merci. Je crois que la question qui se pose c’est essayer de rentrer dans des marchés qui ne sont pas encore ouverts et ainsi de suite. Par exemple, la délégation africaine à l’ICANN, AFRALO/AfrICANN et les représentants viennent parler de l’utilisation malveillante du DNS et de la croissance du marché également. Et c’est là où il y a beaucoup de problèmes aussi, au niveau de l’infrastructure, au niveau de la confiance que l’on a dans l’internet. Donc il faut que l’on conserve le système de nom de domaine, le DNS, qui est le plus sûr, donc il faut trouver l’équilibre dans notre conversation. Et, en même temps, il y a des conversations qui se déroulent depuis longtemps et je crois que l’on revient toujours un peu sur les mêmes sujets parce que cela n’avance pas beaucoup. Donc on a besoin de plus de fluidité, je crois. Je ne veux pas dire prendre parti, mais vous avez parlé d’une certaine utopie. Mais moi, en tant qu’utilisateur final, titulaire de nom de domaine, ce qu’ils

apprécient, c'est difficile en ce moment et ils rencontrent des problèmes.

MICHELE NEYLON Pour moi c'est essentiel, en tant qu'utilisateur final, arriver en ligne, c'est difficile.

JONATHAN ZUCK Vous vous voulez dire vous connecter ?

MICHELE NEYLON Je n'ai pas dit cela, se connecter en ligne, cela devient difficile. Et cela arrive quand on voyage, il y a de pays où on a peu d'accès à internet, le wifi par exemple dans un aéroport va prendre beaucoup d'informations et c'est difficilement acceptable, pourquoi je dois vous donner telle ou telle information ? Ça, ce sont des barrières et des obstacles pour les utilisateurs finaux. Il faut trouver le bon équilibre entre la protection des utilisateurs parce que, très souvent ils ne savent pas ce qu'ils font, et il faut trouver cet équilibre par rapport aux activités criminelles qui sont inacceptables. Mais on ne peut pas se concentrer uniquement tout le temps sur arrêter des personnes, rechercher les abus. Il faut trouver le bon équilibre. Et je sais que ce n'est pas facile. Et beaucoup d'entre nous risquent de perdre leur travail aussi.

JONATHAN ZUCK Merci. James ?

JAMES GALVIN

Bonjour, je suis liaison SSAC auprès du CA. Vous avez parlé d'utopie, d'arriver à une utopie, mais ce dont parlait Michele pourrait devenir un élément d'une campagne sur un cyberespace plus sûr qu'on essaye de développer. On travaille à une campagne de ce type, donc c'est quelque chose qu'on pourrait utiliser, c'est quelque chose qui a été dit pour sécuriser plus le cyberespace pour les utilisateurs finaux.

JONATHAN ZUCK

Je donne la parole à Gabriel.

GABRIEL ANDREWS

J'aimerais répondre à Michele et dire que, sans être alarmiste, on parle de sécurité du public, on parle de la situation que nous avons actuellement, nous avons des chiffres que nous connaissons. Mais j'aimerais offrir une branche d'olivier et je crois qu'on peut travailler de manière plus productive ensemble. Ce que j'aimerais entendre est que l'on résolve ces problèmes qui sont néfastes pour les utilisateurs. Et, d'une manière productive, on peut faire plus et limiter l'utilisation malveillante du DNS et les attaques contre tout le monde dans le monde, y compris nos amis et nos familles. On a besoin de collaboration ici et c'est l'esprit qu'on doit avoir, je dois le reconnaitre. Merci.

JONATHAN ZUCK Merci. Eunice ?

EUNICE ALEJANDRA PEREZ COELLO Merci. Je vais m'exprimer en espagnol. Je pense que cette séance est tout à fait intéressante et ce que vous avez mentionné sur les droits humains, je crois que cela fait participer beaucoup d'éducation et d'information des utilisateurs finaux, trouver des méthodes pour résoudre ou atténuer ces vulnérabilités, ces attaques que nous voyons. Et on ne pense pas véritablement à une manière de faire prendre conscience les utilisateurs finaux. Parce qu'ils utilisent des technologies qu'ils connaissent mal, certaines vulnérabilités qui existent et peuvent émerger à ce niveau. Et je pense que le groupe SSAC pourrait travailler avec l'ALAC pour gérer cette prise de conscience des utilisateurs, prise de conscience renforcée pour limiter ces attaques et avoir des chiffres en décrue. Et c'est important de former les utilisateurs finaux pour qu'il y ait moins d'abus.

JONATHAN ZUCK Oui, tout à fait d'accord. C'est un travail pour nous tous, avec de nombreuses facettes. Reg ?

REG LEVY Oui, je crois que vous avez soulevé quelque chose de tout à fait important à l'ICANN et je crois que la question qui se pose c'est que c'est par exemple l'internet des objets et les situations implicites, par exemple les mots de passe pour le wifi et ça, ça peut avoir un

impact sur votre compte en banque, il y a beaucoup de choses qu'on ne comprend pas. J'ai dû expliquer à mon mari le concept des réseaux wifi invisibles qu'il fallait utiliser ; mais ce n'est pas toujours que l'on peut faire. Ici à l'ICANN, nous avons un mandat spécifique, un cadre de référence limité et il y a des choses que les utilisateurs finaux ne comprennent pas bien. Je crois qu'il faut trouver des solutions à ces problèmes et je ne sais pas comment les trouver véritablement.

JONATHAN ZUCK Merci. Claire ?

CLAIRE CRAIG Bonjour, je suis vice-présidente de l'ALAC. Merci pour cette conversation. C'est plus un commentaire qu'une question et j'apprécie beaucoup écouter les différentes perspectives dans la salle. Ce que je voulais dire c'est que dans la communauté At-Large, ce qui nous préoccupe le plus c'est les intérêts des utilisateurs finaux. Et comme résultat de cela, nous devons avoir une approche plus équilibrée concernant la manière dont les utilisateurs finaux sont impactés quand ils ont accès à l'internet. Et tout particulièrement dans les régions moins avancées et moins desservies. Donc des bureaux d'enregistrement et des opérateurs de registre ont parfois moins de moyens et j'ai apprécié les présentations faites concernant la sécurité publique, parce qu'on a

parlé des véritables menaces qui existent en ce qui concerne les utilisateurs finaux.

Je crois qu'à ALAC et At-Large, c'est ce qui nous concerne au niveau des RALO, nous avons besoin de faire plus de formation et de travailler avec les autres communautés pour s'assurer que les utilisateurs finaux aient le soutien nécessaire.

JONATHAN ZUCK Merci, Claire. Amrita ?

AMRITA CHOUDHURY Oui, sur quoi sommes-nous d'accord ? Utiliser l'internet, protéger les utilisateurs finaux, leurs droits et leurs droits lorsqu'ils sont abusés. Je crois qu'il y a des points communs. Nous pouvons tomber d'accord. L'innovation doit être acceptée.

Donc, que faire en cas d'utilisation malveillante des noms de domaine ? Ça, ce sont des points au niveau du contenu, ça ne nous concerne pas. Mais lorsque l'on sort de cette réunion, les personnes ne comprendraient pas cela. Donc, comment simplifier les choses parce que le cadre des choses est limité. Indiquer nous avons des responsabilités, mais pas toutes, comment expliquer ce que nous pouvons faire au niveau de l'ICANN pour lutter contre l'utilisation malveillante du DNS. Nous voulons absolument respecter la confidentialité et également informer beaucoup les bureaux d'enregistrement et les opérateurs de registre. Je crois qu'il faut articuler cela plus clairement et travailler avec les forces

de l'ordre également. Expliquer ce que nous pouvons faire, tout n'est pas parfait, il faut faire ce qui fonctionne le mieux. Il y a des personnes qui effectuent des abus, il y a des domaines d'où proviennent ces abus et que faisons-nous à ce niveau, comment pouvons-nous agir ?

Voilà ce sur quoi il faut travailler. Et vous avez parlé des droits des utilisateurs, la protection des utilisateurs et des personnes qui sont abusées parce qu'il y a des personnes parfois peu éduquées, je viens d'une région où nous avons des personnes qui arrivent sur internet et qui ne savent pas comment faire, qui contacter, ils n'ont pas de recours, donc il faut les soutenir et qu'ils aient une bonne expérience positive sur l'internet. C'est un problème grave, difficile à résoudre. Mais il faut s'y atteler, en débattre. Que ce soit plus facile dans l'écosystème de l'ICANN de réagir à ces problèmes. Donc on a l'impression que rien n'est fait. C'est l'impression que cela donne. Et, parfois, les problèmes sont mis sous une loupe. Donc je crois qu'il faut voir un petit peu l'impact qu'il y a à la suite de ces problèmes. Ce ne sont pas les chiffres qui comptent, c'est l'impact de cette utilisation malveillante du DNS.

JONATHAN ZUCK Merci, Amrita, il faut en effet se concentrer là-dessus. Merci de votre compréhension.

TIJANI BEN JEMAA

Merci à NetBeacon pour le travail qu'ils font, c'est très apprécié. Le mot clef ici c'est l'équilibre. Oui, les utilisateurs ont besoin d'atténuation de l'utilisation malveillante du DNS parce qu'il faut qu'ils protègent leurs droits en tant qu'utilisateurs. Mais tous les signalements d'utilisation malveillante devraient amener une action, la vérification de ce signalement doit être le premier pas dans cette lutte. On doit rendre cette étape très efficace. C'est un nœud, comme on dit. On ne veut pas un abus de l'atténuation de l'utilisation malveillante du DNS. Donc il faut s'appuyer sur l'équilibre et prendre cela en compte.

JONATHAN ZUCK

Farzaneh ?

FARZANEH BADIEI

Souvent il s'agit plutôt d'un alignement que d'un équilibre. La confidentialité, la liberté d'expression, la sécurité peuvent aussi être utiles pour créer un environnement sûr pour les utilisateurs, pour leur accès. Oui, je l'ai déjà dit, pour nous l'atténuation de l'abus du DNS est très importante, il ne s'agit pas seulement la sécurité de l'utilisateur qui est prise en compte, mais aussi les droits humains. Quand on fait l'atténuation de l'abus du DNS, cela peut empêcher l'accès à un site web et donc ils n'auraient pas accès à certaines connaissances ou informations. Donc quand on parle d'utilisateurs, à la CNCSG, on est intéressé par leur bien-être.

C'est pour vous dire que l'utilisation malveillante du DNS n'en est pas arrivée à un niveau ou l'utilisation de l'internet est devenue impossible. Mais nos politiques et les mises en œuvre que vous allez faire pourraient avoir un impact sur le maintien des noms de domaine, cela deviendra certainement plus difficile, tout le monde pourra aller vers des applications, des plateformes et, de l'autre côté on va dire : pourquoi il y a une concentration médiatique sur tel ou tel endroit ? Parce qu'on rend les choses trop difficiles pour que les personnes aient et gèrent leur propre nom de domaine. On aura rendu les choses trop compliquées.

JONATHAN ZUCK

Je ne sais pas si on avance trop vite dans ce domaine. Des amendements et des contrats ont été mis en œuvre, on a parlé de cela avec la conformité il y a 16 ans ; je ne sais pas si la communauté a surréagi ou alors c'est parce qu'on en parle beaucoup. Mais c'est dur pour moi d'imaginer que nous, au sein de la communauté ICANN, ayons créé un environnement qui est allé trop loin sur ce sujet.

Je vais revenir là-dessus parce qu'on a l'impression que les choses avancent. Quand les choses avancent trop vite, on est en danger de surréagir. Et il y a un micro volant dans la salle, si vous voulez prendre la parole ou poser une question, n'hésitez pas.

Hadia ?

HADIA ELMINIAWI

Merci. J'espère que nous sommes tous d'accord, du moins je pense que nous sommes tous d'accord que la sécurité des utilisateurs finaux, la confidentialité et leur sécurité sont importantes.

Mais pour faire écho à ce qui a été dit, il nous faut une approche alignée et une approche qui va considérer tous ces facteurs. Merci.

JONATHAN ZUCK

Greg ?

GREG SHATAN

Il nous faut éviter d'être trop alarmistes, des deux côtés de cet enjeu, on ne veut pas que ce soit impossible de se connecter à l'internet, mais on ne veut pas non plus que ce ne soit pas sécurisé. Il nous faut un espace qui soit facile, dans lequel on peut opérer en sécurité. Je pense que ce n'est pas un équilibre impossible, mais c'est un équilibre qu'on doit accomplir, atteindre. Il nous faut une facilité d'utilisation sans nécessairement avoir une facilité d'utilisation malveillante. Il nous faut être prudents. C'est ce qu'on disait tout à l'heure, on est en train de dire que tout le monde va aller vers les plateformes, mais vous allez être autant à risque de recevoir du pourriel, d'être piraté. Alors, nous allons continuer à travailler vers cet équilibre dont on parle. Merci.

JONATHAN ZUCK

Quelqu'un d'autre veut prendre la parole ? Très bien. On sait que c'est heure du déjeuner, on doit s'arrêter, mais on a quand même eu une conversation très dynamique et très calme malgré tout.

J'apprécie vraiment la présence de tous et les présentations. Justine, vous voulez dire quelque chose ?

JUSTINE CHEW

Si vous regardez l'ordre du jour, je devais parler pendant 5 minutes, je dois confesser que cette discussion a été tellement riche que j'ai même arrêté de prendre des notes. Je vais un peu régurgiter ce que j'ai entendu jusqu'à présent. On a parlé d'équilibre, on a besoin de communication, alors je pense que c'est ce que font les parties contractantes déjà. Donc plus de communication va nous aider. Et quand il s'agit de la perspective des utilisateurs finaux, à l'ALAC et à l'At-Large, on ne pousse pas les choses à un point non raisonnable. C'est quand même une conversation multipartite.

Mais s'agissant d'une politique liée à l'utilisation malveillante du DNS, dans cette perspective, il faut voir ce que font les bons bureaux d'enregistrement et les opérateurs de registre et il faut voir que les choses sont bien transférées au sein des politiques pour pouvoir protéger l'écosystème de l'internet. Il y aura toujours de mauvais acteurs qui feront de mauvaises choses. Mais je pense qu'on est tous arrivés à la même conclusion, on fait ce qu'on fait pour améliorer les choses. Je pense que tout a été bien décrit aujourd'hui. Merci pour toutes ces suggestions, nous allons prendre tout cela en considération.

Merci à tous les panélistes qui sont venus nous parler aujourd'hui et à tous ceux qui ont contribué à cette discussion très intéressante. Merci.

JONATHAN ZUCK Bon appétit à tous.

[FIN DE LA TRANSCRIPTION]