ICANN68 | Forum de politiques virtuel – Séance plénière : utilisation malveillante du DNS et enregistrements malveillants pendant l'épidémie du COVID-19
Lundi 22 juin 2020 – 13h00 à 14h30 MYT

MARY WONG: Je vais donc demander à ma collègue Ria de lancer la séance, l'enregistrement a commencé.

Bonjour à toutes et à tous. Je crois que Ria est en mode silencieux. Je veux m'assurer qu'on l'entendre. Donc je vous souhaite la bienvenue.

RIA OTANES : Oui, excusez-moi, j'espère que vous m'entendez maintenant ?

BRUCE TONKIN: Oui, tout à fait.

RIA OTANES : C'est parfait. Donc bonjour et bienvenue à cette séance plénière sur les abus du DNS et l'utilisation malveillante des enregistrements. Je suis la responsable de la participation à distance. Cette séance est enregistrée, et nous allons observer les critères de l'ICANN pour les réunions.

Nous allons donc avoir, dans les questions/réponses, la possibilité de poser des questions. Toutes les questions et commentaires doivent être lus à haute voix. Si vous voulez poser votre question ou effectuer verbalement votre commentaire, veuillez lever la main. Nous vous donnerons la permission d'ouvrir votre micro. À ce moment-là vous aurez votre micro, vous indiquez la langue que vous allez parler si ce n'est pas l'anglais.

Nous allons avoir la transcription et l'interprétation aujourd'hui. Pour voir la transcription, vous allez le voir sur la barre d'outils de Zoom. Pour écouter l'interprétation, vous aurez besoin de télécharger l'application. Vous avez plus d'informations dans le programme de la séance. Et nous le mettrons également dans le chat.

Je donne maintenant la parole à Bruce Tonkin.

BRUCE TONKIN: Oui, merci beaucoup Ria. Donc il s'agit d'un suivi que nous allons effectuer depuis la réunion de Montréal l'année dernière.

Donc beaucoup a changé dans le monde depuis Montréal, la manière dont nous travaillons notamment. On travaille depuis chez nous, et la plupart d'entre nous, nous sommes dans nos foyers.

L'année dernière, à Montréal, nous avons entendu parler des contrats qui existent avec les registres et les bureaux d'enregistrement, et les contrats au niveau de l'utilisation malveillante du DNS. Donc les différents suivis, les différents rapports qui existent pour que ces abus

soient tout à fait limités, qu'il y ait des actions entreprises pour gérer cela.

Donc l'ICANN Org a un système en place pour des rapports concernant l'utilisation malveillante du DNS. Nous avons notamment le système DAAR qui existe.

Et nous avons entendu, depuis, qu'il y a un cadre de référence qui a été mis en place par 11 registres et bureaux d'enregistrement pour lutter contre l'utilisation malveillante du DNS, notamment avec ce système de signalement des cas d'utilisation malveillante des noms de domaine.

Nous avons également parlé beaucoup des abus concernant le contenu. Nous avons vu le travail de la CCTRT également, concernant la confiance des consommateurs. Et nous avons entendu parler des représentants des gouvernements concernant l'utilisation malveillante du DNS. Nous avons eu de longues conversations entre différents panélistes et membres de la communauté. Et il y a toute une transcription qui existe par rapport à la dernière réunion qui s'était déroulée à Montréal.

Et nous devions définir mieux les termes, nous devions indiquer ce sur quoi l'ICANN était responsable. Donc définir un petit peu mieux dans toute la communauté ces problématiques, trouver les bonnes parties prenantes pour régler ces utilisations malveillantes du DNS, voir des processus, des mécanismes, pour réagir si on prend par exemple un

nom de domaine et qu'on l'utilise de manière malveillante dans le DNS.

Donc diverses incitations également pour les opérateurs de registre, pour que les meilleures pratiques soient effectuées. Le rôle des contrats par rapport aux meilleures pratiques également. Le niveau de conformité contractuelle, avec l'équipe de conformité de l'ICANN.

Donc, comme suivi, cette séance a été prévue pour notre réunion virtuelle, ICANN 68, et nous avons deux éléments, deux grands segments ou chapitres.

Premièrement savoir ce qu'il s'est passé depuis que nous avons parlé à Montréal. Dans un environnement de travail à la suite de la pandémie Covid19 où beaucoup d'utilisateurs finaux utilisant l'internet depuis leur foyer, ce qui est peut-être moins sécurisé que s'ils étaient au bureau. Ou bien dans des écoles. Ils utilisent des ordinateurs qui ont peut-être des systèmes d'opération avec plusieurs problèmes, pas aussi sécurisés. Moins sécurisé en tout cas. Et ils pourraient être plus susceptibles à des abus du DNS, et des utilisations malveillantes.

Donc nous voulons entendre nos intervenants depuis Montréal. Qu'est-ce qu'il s'est passé depuis Montréal ? Qu'est-ce qu'il y a de nouveau, qu'est-ce qui fonctionne bien, qu'est-ce qui ne fonctionne pas bien du tout.

Et ensuite, durant la deuxième partie de la séance, nous allons parler un peu plus de l'écosystème de l'ICANN, quelles sont les prochaines étapes, qu'est-ce qu'on pourrait mettre en place comme mesure, quel est l'impact que l'on peut avoir sur le problème, un impact tangible. Et, par la suite, nous pourrons répondre aux questions de l'auditoire.

Donc sans plus attendre, je vais donner la parole à Jim Galvin, qui est du groupe des parties prenantes des opérateurs de registre. Jim Galvin, vous avez la parole pour votre présentation.

JIM GALVIN: Merci Bruce. Je m'appelle Jim Galvin, d'Afilias, et je représente donc le groupe des opérateurs de registre.

Donc vous avez des points importants que je veux soulever aujourd'hui, par rapport à l'utilisation malveillante du DNS.

Tout d'abord, je voudrais souligner qu'il y a un cadre de référence volontaire qui existe, c'est un engagement volontaire des opérateurs de registre, avec les bureaux d'enregistrement également. Il y a des personnes qui ont signé cela volontairement pour utiliser ce cadre de référence. Et ce qu'il y a de plus important ici, c'est de définir véritablement l'abus du DNS, l'utilisation malveillante du DNS.

Il y a eu une définition, adoptée officiellement par les parties prenantes, et ça c'est plutôt positif pour la communauté, ça donne une ligne de base tout à fait claire pour les parties [inaudibles] qui

sont tombées d'accord sur des éléments que l'on rencontre dans le système du DNS.

Les abus du DNS sont définis par 5 larges catégories. Nous avons les logiciels, l'hameçonnage, les spams également.

Et je veux donc parler plus particulièrement de cela, de ces pourriels, parce que ce n'est pas le pourriel en tant que tel, non, c'est véritablement un mécanisme de livraison dans le DNS. Donc ça c'est tout à fait différent. Et on ne parle pas d'obligations de lutter contre les pourriels, mais on essaye de vous expliquer ce que ces pourriels peuvent représenter comme utilisation malveillante.

Donc on peut faire une distinction très claire entre l'abus du contenu des sites web et ce qu'il y a de beaucoup plus malveillant au niveau du DNS.

Donc les opérateurs de registre ne peuvent pas tout contrôler, les bureaux d'enregistrement non plus.

Et vous pouvez voir à l'écran un petit peu cet écosystème qui montre, je l'espère clairement, qu'il y a beaucoup de parties prenantes et d'acteurs. Vous avez les opérateurs de site sur la gauche, vous avez les bureaux d'enregistrement, et les titulaires de nom de domaine qui vont travailler avec des prestataires de service internet qui vont être les hôtes de ces noms de domaine. Et les titulaires de nom de domaine passent par des revendeurs.

Mais pour la définition de l'utilisation malveillante du DNS, vous avez en vert les bureaux d'enregistrement et les opérateurs de registre qui gèrent très rapidement les abus, les utilisations abusives.

Donc nous avons des instruments, on peut retirer carrément un nom de domaine du DNS. Et ça, c'est le rôle des opérateurs de registre et des bureaux d'enregistrement.

Mais lorsqu'on est plus au niveau du contenu, lorsqu'il y a un abus au niveau du contenu, et bien là on doit limiter un petit peu les problèmes, lorsque l'on a accès à ces contenus on doit modifier un site web peut-être et retirer le contenu.

Donc on va en entendre parler un petit peu plus, on va principalement parler de la Covid 19 aujourd'hui, de ces abus qu'on a vus depuis la pandémie, depuis l'apparition de la pandémie. On a vu que ce cadre de référence et cet écosystème peuvent être très efficaces. Nous déjà eu une séance un petit peu plus tôt, à l'ALAC. Le GAC a entendu parler de cela également.

Les bureaux d'enregistrement et les opérateurs de registre peuvent beaucoup lutter, efficacement, contre ces problèmes.

Avec la Covid 19 et la pandémie on a eu beaucoup d'utilisation malveillante et d'abus au niveau de l'enregistrement de noms de domaine. Et il y a eu des actions de prises. Parfois elles ont été trop limitées, parfois elles se sont limitées aux abus de contenus dans les sites web.

Nous faisons notre travail en tant que bureaux d'enregistrement et opérateurs de registres. Nous travaillons avec les prestataires de service internet, et nous nous assurons que, dès que possible, on gère les problèmes de contenus abusifs, ou alors s'il y a des représentations de données tout à fait fausses et bien nous agissons là aussi. Nous avons des instruments pour retirer, comme je vous l'ai dit, ces noms de domaine.

Donc voilà les deux points que je voulais soulever aujourd'hui. Je redonne la parole à Bruce et je répondrai à vos questions un petit peu plus tard avec grand plaisir.

BRUCE TONKIN: Merci beaucoup de ce résumé. Nous avons maintenant Graeme Bunton.

GRAEME BUNTON : Et bien bonsoir Bruce, c'est Graeme Bunton. Je suis très heureux d'être ici.

Je suis désolé, il est très tard ici, et ça fait très longtemps que je ne me suis pas coupé les cheveux, et donc je porte une casquette. Et ça fait sens, je crois.

Donc nous allons donc avoir quelques diapos de présentées.

Donc merci Jim d'Afilias. Je suis d'accord avec tout ce que vous avez dit, je vais essayer de ne pas me répéter. Mais vous savez, les bureaux d'enregistrement et les opérateurs de registre sont des partenaires pour lutter contre l'utilisation malveillante du DNS. Et il y a beaucoup d'activités depuis la pandémie de Covid 19. Donc je ne veux pas répéter ce qui a été dit. Mais, insister sur le fait que nous prenons nos responsabilités, nous sommes très alignés comme l'a dit Jim.

Je voudrais prendre quelques minutes pour parler des activités dans le RrSG depuis Montréal. Donc qu'est-ce qu'il y a de nouveau ? A Montréal, on a bien compris que nous devions vraiment creuser un petit peu sur cette utilisation malveillante du DNS.

Donc on a eu un groupe de travail qui s'est formé. On s'est réuni toutes les deux semaines, sauf pendant la période des fêtes. Et ça nous a demandé un petit peu de temps pour trouver des méthodes de travail pour ce groupe, définir nos priorités. C'était assez sensible comme discussion. Donc on devait être tout à fait en confiance entre nous, et nous devions avoir des priorités de définies. Parce qu'il y a beaucoup, beaucoup, de problèmes différents d'utilisations malveillantes du DNS.

Donc on a choisi de faire beaucoup d'éducation au niveau externe, de fournir beaucoup de documents à la communauté, parce que nous pensions qu'il y avait des cibles faciles à atteindre, et que ce serait tout à fait bénéfique.

Donc pour cela, on a publié un guide par rapport aux meilleures pratiques pour effectuer des comptes-rendus sur les utilisations malveillantes du DNS.

Si vous voyez des abus, et bien vous pensez que le bureau d'enregistrement peut faire quelque chose, et bien vous avez ces informations pour agir.

Donc je crois que ça a été très utile comme guide. Et je sais que ça a été utilisé beaucoup par les forces de l'ordre en Europe.

Et nous avons créé également des informations minimums requises pour les demandes de données WHOIS. Donc là, une nouvelle fois, si vous avez besoin d'avoir des informations qui ne sont pas publiques, puisqu'elles sont régulées par le respect de la vie privée et différentes règles et règlements, et bien vous pouvez soumettre un formulaire pour demander, éventuellement, d'avoir ces données WHOIS. C'est pas une garantie, mais c'est une information tout à fait utile.

Tout cela est disponible sur notre site web, RRSG.ORG, je vais mettre tout ça sur le chat.

Et donc ensuite il y a un certain nombre d'activités relatives au Covid, et assez rapidement, il a été clair que nous sommes dans des circonstances tout à fait différentes. Donc nous nous sommes rassemblés, nous avons reparlé des différentes pratiques, des différentes leçons que nous avions tirées et qui pourraient utiles au reste du secteur.

Depuis lors, je pense que nous avons quand même pas mal avancé, mais je ne veux pas répéter ce qui a déjà été dit. Je fais référence à la séance des parties contractantes que nous avons organisée le 11 juin me semble-t-il. J'y ai fait part de certaines données, de certaines démarches qui ont été utilisées pendant cette crise du Covid 19.

Vous l'avez déjà entendu dire, mais il n'y a pas eu énormément d'utilisation malveillante du DNS, mais il y a eu beaucoup d'enregistrements relatifs au Covid 19.

Au sein des groupes des parties prenantes, il y a eu d'excellentes discussions relatives au partage d'information, d'outils, de listes également qui sont très utiles pour les personnes qui n'ont pas nécessairement la capacité à l'interne d'évaluer tous ces enregistrements par eux-mêmes.

Ces outils, ces listes ont également été compliqués à mettre en place, puisqu'il y a eu différents niveaux de qualité. Laureen, Gabe, lors de la séance GAC qui a eu lieu tout à l'heure, ont mentionné toute la communication qui a eu lieu, et cela a été très utile. Nous apprécions énormément ce dialogue ouvert qui a été mis en place.

Nous sommes en phase de résumer ces différentes données, ces différentes expériences. Il y aura une autre déclaration qui sera publiée sous peu.

Donc là, je passe un petit peu à la deuxième partie de la séance, mais nous avons vraiment l'opportunité de travailler de manière assez

sérieuse sur les lacunes, sur les leçons que l'on peut tirer de cette crise, et peut-être réfléchir à ce que nous pouvons faire pour mieux informer le secteur.

Voilà, je vais vous repasser la parole Bruce.

BRUCE TONKIN: Merci Graeme. Nous avons maintenant Laureen Kapin, du GAC, elle est également membre du PSWG et je lui passe la parole.

LAUREEN KAPIN : Merci Bruce. Bienvenue à tous. Je suis avocate à la FTC et je m'occupe de la protection du consommateur. Vous voyez ma petite décharge.

Je vais maintenant vous faire part de mes commentaires, qui ne sont pas nécessairement le positionnement officiel de la FTC. Je suis donc co-présidente du groupe de travail sur la sécurité publique au sein du GAC.

Je voulais vous faire part de certaines informations que la FTC a rassemblées sur les plaintes relatives au Covid19, pour souligner un petit peu l'ampleur de ces questions. Et je voulais mettre l'accent sur une chose. Il s'agit d'informations d'ordres générales sur les plaintes relatives au Covid 19. Et il n'y en a sans doute qu'une partie qui a trait à une utilisation malveillante du DNS. Mais c'était pour vous donner une idée de l'ampleur de cette question.

Mon agence rassemble les plaintes des consommateurs aux États-Unis, mais également de consommateurs du monde entier.

Nous avons beaucoup d'informations qui sont disponibles, publiquement, sur ce que nous collectons et ce que nous observons.

Vous voyez là un diagramme qui représente le total de toutes les plaintes, donc plus de 100 milles, depuis janvier – et vous voyez la ligne à droite qui vous montre qu'il y a eu un pic au mois d'avril – mais malgré tout le niveau demeure élevé. En termes de quantité d'argent perdu, cela représente plus de 68 millions de dollars. Et pour le consommateur, 289 dollars en moyenne.

Donc il y a des programmes qui permettent de fournir de l'argent aux personnes qui sont au chômage, donc des programmes gouvernementaux, et comme vous le savez, à chaque fois qu'il y a ce type de choses, et bien il y a le risque de problèmes, de plaintes et d'utilisation malveillante.

Diapositive suivante.

Je souhaitais également évoquer les méthodes de communication pour les acteurs malveillants, la manière dont ils contactent les gens. Donc il y a le téléphone, mais en deuxième et troisième position, vous avez les sites web et l'email. Et donc, bien évidemment, ceci peut être lié à une utilisation malveillante du DNS.

Je souhaite mettre l'accent d'abord sur ce qui fonctionne bien. Parce que la deuxième partie de la discussion aura trait à ce qui est plus compliqué, à ce que l'on peut améliorer.

Mais comme Graeme l'a mentionné, et j'aimerais mettre l'accent là-dessus, les organismes d'application de la loi ont bien collaboré avec les bureaux d'enregistrement et l'ICANN. Nous avons pu collaborer lorsque les noms de domaine semblaient trompeurs ou relatifs à du contenu troublant. Nous avons donc pu mettre en place un dialogue avec les bureaux d'enregistrement sur ces questions. Nous avons donc un lien direct, une communication directe, pour faire le suivi.

Et donc avoir cette communication ouverte est tout à fait bienvenu et bénéfique. Et ceci est un exemple de la manière dont on peut collaborer pour lutter contre l'utilisation malveillante du DNS.

Nous savons que plusieurs des bureaux d'enregistrement ont, de manière proactive, fait un dépistage de ces noms de domaine relatifs au Covid 19, et qu'ils ont établi la communication avec les organismes d'application de la loi. Donc la communication va dans les deux sens, ce qui est tout à fait utile.

Nous communiquons avec les bureaux d'enregistrement, et eux communiquent avec les organismes d'application de la loi.

Ce dépistage initial représente un exemple parfait de ce qui peut bien fonctionner dans le domaine de l'utilisation malveillante du DNS.

Voilà, je vais vous repasser la parole Bruce.

BRUCE TONKIN: Merci Laureen. C'est toujours très bien quand on remarque que les choses fonctionnent. Nous avons Peter Van Roste, de la ccNSO. Peter, vous êtes là ?

PETER VAN ROSTE : Oui, bonjour Bruce. Je suis bien là. Merci beaucoup. Je suis responsable de CENTR.

Au cours des quelques minutes à venir, je vais vous parler des constatations de mes collègues dans la région. L'APTLD, l'AFTLD, etc. ont également fait part d'informations lors d'un webinaire il y a deux semaines de ça.

Je crois que pour la plupart des personnes qui sont présentes aujourd'hui lors de cette réunion, vous savez que les ccTLD ne font pas partie du cadre d'utilisation malveillantes. Les politiques ccTLD sont établies au niveau local, pas au niveau de l'ICANN.

Mais, ce que nous avons observé pendant la crise du Covid c'est certains parallèles assez intéressants que nous pouvons noter entre ces deux mondes qui sont en fait tout à fait similaires.

Donc en ce qui concerne l'utilisation malveillante relative au Covid 19, au sein de CENTR, nous avons 12 fournisseurs de ccTLD qui nous ont donné leurs données de janvier à avril. Il y avait de grands bureaux

d'enregistrement et de petits bureaux d'enregistrement dans ce groupe.

Nous pouvons en fait utiliser les noms Covid, Corona, etc. pour identifier les noms. Donc sur les 6 000 que nous avons identifiés, il n'y en a que 1 600 qui étaient à un contenu élevé. Sur ces 1600, 100 ont été confirmés parmi les ccTLD participants, donc confirmés comme étant des utilisateurs malveillants.

Mes collègues de Nominet nous ont dit que 3 au Royaume-Uni et 6 au Danemark étaient concernés. Donc même constatation que ce qui a été identifié dans le domaine des ccTLD.

Le problème que nous avons eu c'est que nous n'avons pas vraiment pu collaborer au niveau des statistiques.

Apparemment le problème était beaucoup plus élevé que ce que nous avions pensé, donc nous avons perdu du temps. Nous continuons de travailler avec les organismes d'application de la loi et autres partenaires pour voir sur quoi nous devons focaliser notre attention.

Ce qui a bien fonctionné, c'est que nous avons collaboré avec les autorités locales, que ce soit les autorités de santé, d'application de la loi, etc. Ça a vraiment été la clé pour identifier, pour cibler les noms qui étaient utilisés de manière malveillante.

D'une manière générale, et pour conclure ce que font les ccTLD dans cette période Covid, en termes de protocoles comment peut-on comparer ceci avec le cadre d'utilisation malveillante, et bien il y a eu

vérification lors de l'enregistrement, donc les circonstances extraordinaires nécessitent beaucoup de travail. Mais donc les enregistrements ont parfois été faits de manière manuelle, parfois de manière automatique. Et puis il y a eu vérification de l'exactitude. Donc les titulaires de noms de domaine ont augmenté la précision des données fournies. Et autre chose, la collaboration – je l'ai déjà dit – avec les autorités locales. Et pour nous ça a vraiment été la clé.

Voilà, c'est tout. Merci.

BRUCE TONKIN: Merci beaucoup Peter. C'est toujours intéressant d'avoir la perspective des gTLD et des ccTLD, parce qu'il y a effectivement beaucoup de points communs.

Nous avons comme intervenant suivant dans ce segment Jonathan Zuck du comité consultatif de l'At-Large.

JONATHAN ZUCK: Je suis très heureux d'être ici, merci.

Diapositive suivante. Donc ce sont des enregistrements qui sont plus susceptibles d'être à utilisation malveillante.

Diapositive suivante.

Donc un petit exemple d'hameçonnage qui a eu lieu en Italie, il y a un email qui a été envoyé avec divers organismes italiens qui indiquait

donc : étant donné le nombre d'infections identifié dans votre région, l'Organisation mondiale de la santé a préparé un document qui inclut des précautions nécessaires pour la lutte contre l'infection de Corona Virus. Mais en fait, lorsque vous ouvrez le document Word et que vous suivez les instructions, et bien c'est un logiciel malveillant qui s'installe sur la machine et cela a causé beaucoup de problèmes pendant la crise.

Donc je ne vais pas, je ne souhaite pas minimiser ce qu'il se passe pendant la crise, mais je crois que nous sommes toujours confrontés avec la question d'une utilisation malveillante systémique, avec différents acteurs, et je crois qu'il nous faut essayer de voir s'il y a un moyen de s'occuper de ces problèmes de manière acceptable pour les bons acteurs. Parce que nous savons qu'ils sont nombreux dans la communauté de l'ICANN.

Voilà, je vous repasse la parole Bruce.

BRUCE TONKIN: Merci Jonathan. Bien, donc je pense que nous allons maintenant passer à la prochaine séance, pour une question de temps.

Je vois qu'il y a des questions qui apparaissent, donc peut-être que nous pouvons y répondre une fois que nous aurons entendu les autres orateurs.

Il y a beaucoup de choses qui ont été dites, on a dit ce qu'il s'était passé depuis Montréal, ce qui a marché, ce qui n'a pas marché. Donc

les prochains orateurs vont nous dire ce que fait la communauté à ce propos, ce que l'on peut faire pour marquer la différence.

Bien donc je vais commencer par Mason Cole, du groupe des parties prenantes commerciales.

MASON COLE: Bien, merci, merci à tous. Je voudrais commencer par dire bravo à ce qui a été fait auparavant par les parties contractantes dans le cadre du Covid. C'est bien de voir qu'il y a de bons acteurs qui travaillent. Ce que nous affrontons c'est une situation dans laquelle les utilisations malveillantes du DNS étaient vraiment un problème.

Prochaine diapo.

Bien, donc quelques faits concernant l'utilisation malveillante du DNS. On sait que c'est un problème. Et le Covid a augmenté tout cela. Comme toujours dans le cas de catastrophes.

En tout cas, le thème commun est que le DNS est utilisé pour des objectifs illicites, illégaux.

Prochaine diapo.

Quelques faits concernant l'utilisation malveillante du DNS. Il augmente, vous pouvez voir les chiffres ici. On a estimé que le cyber délit va coûter à l'économie mondiale plus de 6 milliards de dégâts. Et

beaucoup de choses sont dues donc à cette utilisation malveillante du DNS.

Et je vous présente ici les résultats d'une association qui montre comment ces utilisations malveillantes sont un problème, par exemple pour les pharmacies. Il y a beaucoup de pharmacies illégales. Et ces bureaux d'enregistrement montrent qu'ils cachent certaines personnes qui agissent de manière illégale.

Voyons un petit peu il y a quelques années ce qu'il s'est passé. Ici on voit une tendance, avec une augmentation, dans le cas de catastrophe. Dans ce cas-là c'était une tornade. Et vous voyez qu'il y avait des noms de domaine qui n'étaient pas toujours fiables.

Prochaine diapo.

Ici, voilà les tendances pour Covid 19. Le Covid 19, voyez de nouveau ce pic à l'époque de la pandémie.

Prochaine diapo.

Ici, voilà, c'est ce que je vous disais tout à l'heure, il y a des cas ici, aux États-Unis, on peut voir que c'est une tendance pour les noms de domaine qui sont enregistrés et qui sont liés à ces situations.

Prochaine diapo.

Alors, j'ai contacté plusieurs compagnies pour parler de cet abus du DNS, cette utilisation malveillante du DNS, et j'ai reçu des

informations de Microsoft, que vous voyez ici. Le Covid 19 a augmenté l'efficacité d'attaque contre la cybersécurité, parce que les personnes qui travaillaient à l'extérieur des sauvegardes des compagnies ont pu attaquer, et il y avait donc la possibilité d'attaquer le DNS. De fait, j'ai constaté à travers Microsoft qu'entre Mars et le 10 juin, le 16 mars et le 10 juin, il y a eu toute une série d'attaques. 4 000 dont ont été indiquées.

J'ai aussi constaté certaines informations qui ne sont pas dans cette présentation, et je les ai trouvées dans une autre source, depuis le mois de mars, 261 domaines ont eu des problèmes liés au Covid, sur Facebook, des noms comme fbcovidcare, covid19.com… Vous voyez donc ce type de noms qui ont été utilisés à ce moment-là.

Donc le problème augmente et ICANN Org n'a pas les outils pour combattre ce comportement envers ces bureaux d'enregistrement malhonnêtes. Il y a des bonnes choses qui sont faites, mais il y a aussi de gros problèmes, des personnes malhonnêtes qui sont là. Et le résultat est une tragédie, et tout le monde est encouragé à faire ce qu'il peut.

Alors, qu'est-ce qu'on peut faire ? On ne peut pas affronter ce type de situation de manière réactive. On ne peut pas mettre en place des attitudes proactives. Donc je dirais qu'il faut utiliser des outils réels pour combattre ces utilisations malhonnêtes.

Les personnes qui sont volontaires sont fantastiques, mais nous avons besoin de techniciens également. Donc nous pouvons utiliser…

Pardon, diapo antérieure.

Nous pouvons analyser des outils comme par exemple le Congrès des États-Unis, qui a été actif et utile, et institutionnaliser ce type de processus à travers des contrats.

Nous savons qu'il y a toujours de bons acteurs, qui font de bonnes choses, mais nous devons pouvoir aussi avoir des outils pour lutter contre les personnes malhonnêtes.

Merci j'ai terminé.

BRUCE TONKIN: Merci. Le prochain orateur est le représentant de SSAC, Jeff Bedser, comité consultatif de sécurité et de stabilité.

JEFF BEDSER: Bien, bonjour, je suis Jeff Bedser, du Comité consultatif de sécurité et de stabilité, le SSAC.

Notre rôle est de lutter contre l'utilisation malveillante du DNS, et je dirais que nous pensons que la communauté est au point où on peut dire qu'il y a un accord pour dire que l'abus contre les consommateurs est un problème.

Il a été abordé de différentes manières au sein de la communauté. Des séances de ce type montrent bien qu'il y a du progrès dans ce sens.

Mais nous devons analyser cela, essayer de trouver un cadre pour les pratiques efficaces, pour des résolutions qui luttent contre ces utilisations malveillantes dans l'ensemble de l'écosystème et du modèle du DNS. À travers des manières de lutter contre ce type d'utilisations malveillantes directement.

Par conséquent, comme cela a déjà été dit par d'autres intervenants, comme Jim Galvin et Graeme, la catégorisation de ces utilisations malveillantes a été établie, du point de vue technique, quel type d'utilisation malveillante des contenus, dans quels domaines doit-on travailler, qu'est-ce qui doit être fait…

Mais une des choses en tout cas que l'on doit faire, sur laquelle on doit travailler, ce sont les normes de preuve. Dans l'écosystème, au sein de la communauté, chaque acteur a différentes normes, a différents standards, dans les manières d'analyser les preuves pour démontrer qu'il y a eu une utilisation malveillante des domaines. Et cela rend les choses compliquées quand on demande à une partie de, par exemple, signer un contrat, et avec des utilisateurs finaux, pour enregistrer un domaine.

Donc il faut se mettre d'accord pour que ces normes soient standardisées, soient normalisées.

Et une des pratiques de signalement des utilisations malveillantes efficace, parce que les pratiques doivent avoir un point commun concernant le type d'utilisation malveillante qui, quel est le contact qui doit s'occuper de ce problème pour avoir un résultat rapidement.

Donc faire une cartographie pour permettre que les rapports, les signalements de ces utilisations malveillantes soient faits auprès des forces de l'ordre, du public, des différentes entités qui s'occupent de cela. Savoir où on doit aller lorsqu'on veut porter plainte pour démontrer que ce type d'utilisation malveillante a eu lieu.

Par ailleurs, il doit y avoir des moyens, des voies d'escalade. Si l'on regarde, si l'on essaye de comprendre si une partie est la bonne pour aborder ce type de problème, si elle ne répond pas, si elle se refuse à répondre, à ce moment-là, il faut permettre une résolution. Dans le cas d'un domaine qui a été utilisé de manière malveillante, quelle est la possibilité d'escalader, comment passer au prochain organisme et comment gérer tout cela.

Et ensuite on a les délais raisonnables lorsqu'une partie ne sait pas quel est le moment raisonnable pour revenir en arrière, et si on n'a pas eu une réponse à qui on doit s'adresser.

Et, à ce moment-là, on doit… Il y a beaucoup de groupes de parties différentes qui se consacrent, il y a différents acteurs dans cet écosystème qui font qu'il est facile d'être enregistré et de trouver une protection.

Donc il y a les données d'enregistrement, mais ce n'est pas nécessairement le titulaire de noms de domaine, cela peut être un fournisseur. Donc tous ces éléments font partie de cet écosystème, et donc la capacité d'aider pour avoir une résolution rapide d'une

utilisation malveillante d'un nom de domaine, c'est quelque chose qui n'est pas toujours évident.

Bruce, je vous repasse la parole.

BRUCE TONKIN: Merci Jeff. Je présente maintenant Brian Cimbolic du Groupe des parties prenantes des opérateurs de registre.

BRIAN CIMBOLIC: Bonjour à tous, je m'appelle Brian Cimbolic. Je suis responsable du contentieux à PIR et je m'occupe également de notre programme.

Donc si l'on regarde un petit peu l'avenir, qui est le thème de cette deuxième partie, je crois qu'il y a plusieurs choses sur lesquelles il nous faut nous concentrer.

Tout d'abord, la poursuite du dialogue entre les parties contractantes et d'autres parties prenantes dans la communauté de l'ICANN sont des choses très importantes. Les gens disent : oui, c'est vraiment dommage, ce travail entre les bureaux d'enregistrement, les opérateurs de registre et les organismes d'application de la loi allait bien, mais le Covid a un petit peu interrompu ceci. Et je ne pense pas que ce soit juste.

Au cours des 5 années passées, je crois qu'à mon avis il y a eu d'excellentes choses qui ont été faites entre les organismes

d'application de la loi, les bureaux d'enregistrement et les opérateurs de registre. Il y a le cadre d'identification des menaces à la sécurité, c'est un document qui a été rédigé entre le PSWG et les opérateurs de registre. Il y a tout ce qui est relatif aux abus contre les enfants. Avec l'expérience, la sagesse, de différents organismes d'application de la loi, toutes leurs connaissances là-dessus. Et le cadre pour s'occuper des utilisations malveillantes du DNS.

Et tout ceci a lieu parce qu'il y a un réel désir des parties contractantes d'identifier le travail à effectuer sur ce problème. Il n'y a pas une seule chose qui ait inspiré ce travail. C'est plusieurs éléments.

Donc ce dialogue qui se poursuit, la discussion qui se poursuit avec le SSAC, tout ceci sont utiles. Plus nous comprenons ce qui est compliqué pour les uns et les autres, moins nous allons ne pas nous comprendre, ce qui souvent se produit dans ce type de situation.

Deuxièmement, Jim a mentionné le cadre pour traiter les utilisations malveillantes, qui s'est beaucoup élargi. Nous avons commencé avec les bureaux d'enregistrement et les opérateurs de registre. Et maintenant nous avons plus de 50 parties contractantes qui se sont engagées par rapport à cette définition de l'utilisation malveillante et qui s'engagent à reconnaitre, à identifier l'utilisation malveillante du DNS et, également, les actions les plus nocives comme la traite d'enfants ou la pédophilie.

Ensuite, je crois qu'il faut être créatif. Que peuvent faire les bureaux d'enregistrement, les opérateurs de registre, pas forcément dans tout le DNS, mais peut-être sur un enregistrement, que peuvent-ils faire ?

Alors, comme exemple – diapositive suivante s'il vous plait – ce n'est pas une initiative du CSG, mais c'est quelque chose qui a été mis au point par le PIR. Il s'agit de l'indice de performance de qualité. Et, en fait, c'est une motivation financière qui est donnée au bureau d'enregistrement s'ils suivent certaines méthodes d'enregistrement. Donc, par exemple, le taux d'abus, le taux de renouvellement, l'utilisation de domaine.

Et donc, récemment, les taux d'abus… Alors ce que je veux dire par là c'est le pourcentage d'abus créé par rapport au nombre de domaines créés. Donc il faut qu'un seuil spécifique soit atteint et c'est une manière donc de récompenser les bons bureaux d'enregistrement, par rapport à cette utilisation de domaine.

Si les bureaux d'enregistrement ne remplissent pas ces critères ils ne peuvent plus participer. Et donc on voit maintenant que les différents acteurs qui, peut-être, n'étaient pas nécessairement très actifs pour gérer ces abus, de plus en plus ces acteurs nous demandent de voir comment ils peuvent mieux gérer la situation.

Et donc, autre chose que j'aimerais dire, et nous en sommes fiers, s'il y a d'autres opérateurs de registre qui sont intéressés à adopter ces [QPI], et bien nous sommes là pour vous aider à mettre en œuvre une version de ce programme qui fonctionne pour vous.

En termes de revente, c'est également quelque chose qui est intéressant pour les bureaux d'enregistrement, ceci incite les comportements positifs, et donc nous aurons cette conversation avec les bureaux d'enregistrement et les opérateurs de registre qui le souhaitent, ainsi qu'avec toute autre personne.

Merci beaucoup.

GRAEME BUNTON : Bruce, je crois que vous êtes en mode silencieux.

BRUCE TONKIN: Oui, donc merci beaucoup de ces perspectives que nous avons entendues, c'était extrêmement intéressant.

GRAEME BUNTON : Oui, merci. Oui, je vais essayer d'être rapide.

Donc pour revenir un petit peu sur notre groupe de travail, nous avons noté que nous avons besoin de plus de temps et nous avons besoin de plus de ressources. Et nous avons besoin de plus de temps pour faire notre travail, et peut-être qu'on peut avoir le soutien du personnel de l'ICANN, ça pourrait être très utile.

Plus largement, en ce qui concerne les abus du DNS en général, je crois qu'il y a une ligne claire par rapport à l'utilisation malveillante du

DNS, et je crois que c'est une très bonne première étape. Il y a encore beaucoup de recherches qui se font.

On a besoin de données de qualité sur ces utilisations malveillantes. Et on a un exemple de mauvaises données qui existent et vraiment qui ne servent à rien pour régler les problèmes.

Ce que l'on peut faire maintenant, c'est avoir une définition pour notre secteur, et à partir de là, nous serons en mesure de voir quels sont les attributs partagés et les caractéristiques partagées par les mauvais acteurs, comment ils agissent. Et une fois qu'on aura identifié ces attributs, et bien là on pourra trouver les outils pour lutter contre cela. Mais je crois qu'on doit commencer à ce niveau-là.

NON IDENTIFIÉ : Oui, je vois que vous êtes là aussi avec un micro éteint.

BRUCE TONKIN: Merci beaucoup Graeme. Nous avons Laureen qui va nous parler un petit peu de son point de vue.

LAUREEN KAPIN : Donc moi je vais passer à la diapositive numéro 5. Oui, la 5 de ma présentation. Voilà très bien. Donc qu'est-ce que l'on peut améliorer ?

Donc, pour préfacer cela, j'aimerais revenir sur deux points qui ont été effectués par Jim Bladel et Jonathan Zuck, les deux J, qui nous ont dit

qu'on parle beaucoup de règles et de règlements pour les mauvais acteurs, mais on a peut-être besoin de plus de règles pour convaincre les mauvais acteurs, ou limiter les mauvais acteurs plutôt.

Jonathan Zuck a souligné que l'autre partie de l'équation c'est les mesures proactives qui peuvent être prises pour véritablement mettre de côté et identifier rapidement et mettre de côté ensuite ces mauvais acteurs néfastes. Donc je crois que ça peut être un concept tout à fait utile.

Donc en ce qui concerne l'amélioration possible, ce que l'on peut utiliser comme écran, si vous voulez, c'est d'avoir des canaux dédiés pour gérer ces abus du DNS et ces menaces sur la sécurité du DNS. Avec des contextes très spécifiques, avec des communications rapides, et agiles. Donc ça, ce serait un excellent outil dans notre arsenal.

Et un autre concept tout à fait important, et une nouvelle fois c'est dans la catégorie des écrans de protection, c'est dès le départ s'assurer que les données qui sont collectées sur les personnes qui veulent enregistrer des noms de domaine, et bien il faut s'assurer que ces personnes n'aient jamais été déjà des acteurs malveillants. Donc bien vérifier qui ils sont, il faut qu'il y ait des vérifications à ce niveau qui soient efficaces. Parce que cela permettra de limiter donc ces mauvais acteurs et ils iront voir ailleurs, tout simplement.

Et je crois que ça, ça peut être quelque chose qui protège beaucoup.

Ce dont on a besoin également, c'est vraiment que les obligations contractuelles soient respectées, qu'elles soient très, très claires pour les nouveaux gTLD, et ce dès le départ. Mais qu'elles aillent plus loin encore ces obligations contractuelles. Il faut qu'elles aient plus de force. Et il faut qu'il y ait des clauses dans ces obligations contractuelles qui soient tout à fait solides et qui précisent quelles vont être les mesures de prises et les conséquences si on ne prend pas ces mesures.

C'est uniquement lorsque les obligations contractuelles arrivent à ces niveaux de clarté, et à ces seuils que la conformité de l'ICANN aura les outils nécessaires pour véritablement avoir des activités robustes.

Donc au niveau des outils, je crois que là, une nouvelle fois, c'est quelque chose de très utile.

Donc je continue avec la diapositive suivante, qu'est-ce que nous aimerions avoir ?

Alors, là, si on avait une baguette magique, si on pouvait transformer le monde comme nous voudrions qu'il soit, et bien s'il y avait des incitations pour encourager les bons comportements, nous avons vu des exemples de carottes. On a besoin de plus de carottes je crois.

Les incitations peuvent bien fonctionner pour encourager les comportements positifs. Ça peut être au niveau financier. Il peut y avoir tout type d'incitations qui existent. Et cela permettra de s'assurer qu'il y aura une bonne précision au niveau des noms de

domaine. Et si on n'obtient un très haut niveau de précision, là on pourra avoir des récompenses peut-être.

Et il faut faire très attention quand il y a des enregistrements en vrac, en grand nombre en même temps. Ça c'est très souvent douteux. C'est vraiment une alerte qui est lancée. Et là on doit étudier de très près ces demandes pour enregistrer de nombreux noms de domaines en même temps.

Donc ce que j'aimerais avoir aussi comme outil, et ça c'est une recommandation de la CCT, pour qu'il n'y ait pas de problèmes systémiques d'abus, systémiques, qui se déroulent avec certains opérateurs de registres, ou certains bureaux d'enregistrement, ce serait vraiment une interdiction de vol, comme on l'a dans le domaine aérien, et des listes noires que nous pourrions avoir.

Donc s'il y a véritablement un bureau d'enregistrement qui a été identifié comme continuellement s'engager dans des conduites illégales, et bien là, à ce moment, on doit l'observer de très près lorsqu'il veut enregistrer des noms de domaine, pour qu'il n'y ait pas, de manière répétitive, ces comportements abusifs.

Donc merci beaucoup, je redonne la parole.

BRUCE TONKIN: Merci beaucoup Laureen. Nous avons notre dernier intervenant, c'est David Conrad d'ICANN Org.

DAVID CONRAD: Oui, je suis responsable de technologie à l'ICANN, et je vais maintenant vous présenter ce qu'ICANN Org peut effectuer au niveau stratégique pour être véritablement dans la même direction que tout ce qui a été dit, de toutes ces initiatives.

Donc, un effort que nous avons engagé récemment, c'est d'avoir plus de sécurité, plus d'outils d'enregistrement, et donc pour limiter un petit peu la limite des enregistrements malveillants et de l'hameçonnage, et vraiment avoir des outils pour qu'il y ait des rapports et des comptes-rendus de confiance pour les bureaux d'enregistrement.

Donc, ça c'est un outil que nous avons bâti depuis la Covid 19, et je crois que c'est quelque chose qui pourrait s'appliquer à diverses situations que nous connaissons, et identifier donc de cette manière des noms de domaine associés à des abus, à une utilisation malveillante, avec de l'hameçonnage notamment.

Donc nous travaillons également avec la communauté, et nous essayons de mieux définir les rapports d'activité d'utilisation malveillante du DNS que nous avons. Et ça fait à peu près un an que nous travaillons à cela, mais on a toujours un manque de compréhension au niveau des données. Que signifient ces données ? Et il y a eu diverses demandes de données plus détaillées, de plus de statistiques, de plus de chiffres et de manière de collecter ces statistiques. Donc on essaye d'y travailler beaucoup plus à l'avenir.

Nous avons commencé également à travailler avec les ccTLD, au niveau de leur infrastructure. Pour les ccTLD ils sont très intéressés comme vous le savez par un protocole d'accord qui permettrait d'obtenir les données nécessaires au niveau du système DAAR et des rapports DAAR. C'est parfois difficile parce que les ccTLD s'inscriraient sur une base volontaire. Et elles veulent faire un bon travail et s'assurer qu'elles sont toute à un niveau qui permet d'avoir des résultats concluants.

Donc tout cela serait inclus dans le rapport DAAR, ce qui n'est pas toujours facile. Nous essayons de trouver la meilleure manière d'agir.

Et puis il y a également un outil qui, en tant que communauté, vous fournit des informations sur les anomalies. Dans le cadre de nos efforts à l'interne, nous avons essayé d'identifier ces anomalies et de nous adresser à ces acteurs pour solutionner le problème de cette anomalie.

Si vous regardez à droite sur le diagramme, vous pouvez voir ce que j'ai encerclé en rouge, ce sont dons des anomalies. Ce sont vraiment des choses qui sortent de ce qui est typique pour d'autres domaines. Et il y a des raisons à ceci. Ça peut être des raisons financières ou autre.

Mais nous avons connu certaines réussites, nous avons contacté les registres qui, justement, présentaient ces anomalies, nous les avons aidés à identifier les problèmes et à les solutionner.

Donc il y a également une initiative de facilitation de la sécurité du DNS. L'idée c'est de fournir un ensemble d'informations, avec de meilleures pratiques, et de promouvoir ces meilleures pratiques dans la communauté, en se focalisant sur l'amélioration de l'écosystème du DNS, sa sécurité en particulier, dans un contexte assez large. Pas seulement au niveau du bureau d'enregistrement et de l'opérateur de registre, mais de manière plus large. Donc l'écosystème du DNS dans son ensemble.

Dans le contexte de la conformité, l'idée c'est de mettre en œuvre les différentes obligations. La conformité s'occupe des plaintes en se focalisant sur l'utilisation malveillante du DNS en utilisant les données qui proviennent de différentes sources. La conformité, bien évidemment, connait le rapport DAAR et peut obtenir d'autres données, mais il y a également des données auxquelles la conformité a accès, les plaintes qui sont envoyées, et tout ceci a un effet de signalement qui permet d'identifier ces acteurs et de cibler les actions.

Du point de vue stratégique, l'ICANN Org souhaite faciliter les discussions en cours relatives à l'utilisation malveillante du DNS, il faut clarifier les rôles des titulaires de nom de domaine par rapport au rôle des parties contractantes et au rôle de l'ICANN.

Une des demandes constantes que l'on reçoit c'est que l'ICANN doit parfois sortir de son rôle, de ce qui est défini dans les statuts. Et de toute évidence, nous ne pouvons pas le faire. Mais le plaignant n'a pas d'alternative, n'a pas d'autres options pour s'occuper de son problème. Donc l'idée c'est de fournir des ressources, des

informations, de manière à ce que les personnes que l'ICANN ne peut pas aider puissent envoyer leur plainte autre part, et donc l'idée c'est de pouvoir les aider à rediriger leurs efforts.

Nous avons mis en place un certain nombre de protocoles d'entente, avec [Cert], avec [GTA], et ces protocoles d'entente font partie d'un effort à long terme. Et nous souhaitons donc faciliter la communication entre les organismes d'application de la loi, les bureaux d'enregistrement, les opérateurs de registre, de manière à fournir plus d'informations sur le rôle de l'ICANN, sur ce que nous pouvons faire et ce que nous ne pouvons pas faire. Et, en fin de compte, lorsque la communauté en arrive à un consensus par rapport à ce que fera l'Org, et bien peut-être qu'il sera question de mise en application des contrats. Tant que ceci ne sera pas compris, et bien ceci représentera pour nous un enjeu. Le problème que nous avons actuellement c'est l'interprétation des contrats. Parfois ce que certaines personnes considèrent comme abusif ne le sont pas pour d'autres.

Donc c'est une des choses que nous souhaitons clarifier, grâce à l'aide de la communauté avec le temps.

Je repasse la parole à Bruce.

BRUCE TONKIN: Merci. Nous avons quelques personnes qui ont levé la main parmi les participants, donc je vais passer la parole à Lori Schulman. On va demander au personnel d'allumer le micro de Lori.

LORI SCHULMAN : Oui, en fait j'ai reçu une réponse dans le chat par rapport à ma question. Les taux d'utilisations malveillantes qui sont peu élevés et leurs mesures me préoccupaient. Ce que j'entends chez les propriétaires de marques de commerce, c'est qu'on voit des pics, et dans le chat, ce qui a été indiqué, c'est que le mot de Covid, Covid en lui-même n'est pas enregistré, mais Covid est rattaché à certaines choses, et ceci est préoccupant pour les marques et pour le public en général.

BRUCE TONKIN: Merci Lori.

La personne suivante sur la liste, c'est Georgios Tselentis. Je ne sais pas si j'ai bien prononcé votre nom, mais allez-y Georgios.

Est-ce qu'on pourrait allumer le micro de Georgios pour qu'il puisse parler ?

Alors, je vais passer la parole à Jannett, qui a levé la main. Jannett ? Allez-y, posez votre question.

Alors, ça ne fonctionne pas. Nous allons passer au forum en ligne. Le personnel va nous lire la question je crois, c'est comme ça que ça fonctionne ? Ou alors est-ce que c'est à moi de le faire ?

RIA OTANES : Je vais lire la question. Est-ce que les agences ont pris en compte la possibilité de concevoir un processus sécurisé pour utiliser les nouvelles technologies de DNS, par exemple un portail de paiement de Blockchain, pas seulement pour les États-Unis, mais également quelque chose qui pourrait être utilisé autre part ?

LAUREEN KAPIN : Je pense que cette question est pour moi. J'étais en train de taper la réponse dans le chat.

Mon agence n'est pas impliquée dans la distribution de paiement de ce type, donc je ne peux pas vous en parler. Mais par contre, ce que je peux vous dire, c'est que de manière très large il a été indiqué que certains des systèmes utilisés - et je crois que c'est de ça que vous souhaitez parler, dans le cadre de ces paiements - étaient susceptibles ou plutôt donnaient lieu à la confusion. Les enveloppes avaient l'air d'être du pourriel, donc elles étaient jetées. Ou alors, les gens étaient contactés soi-disant par des personnes qui disaient : nous avons votre argent du gouvernement dans le cadre du stimulus, mais nous avons besoin d'informations supplémentaires, etc. Et donc les informations personnelles étaient communiquées, ce qui de toute évidence créait un risque d'usurpation d'identité.

Donc je n'ai pas de réponse spécifique à votre question, mais je crois que, d'une manière générale, il faut mieux réfléchir à la manière dont ces paiements sont effectués, de manière à ce qu'ils puissent être faits sans donner lieu à des possibilités de fraudes ou d'usurpations.

BRUCE TONKIN: Merci Laureen. Nous allons prendre la question suivante, de Fabricio.

RIA OTANES : Fabricio : les mesures volontaires sont un bon début, mais pas une réponse à long terme. Comment peut-on s'assurer que certains bureaux d'enregistrement qui ne font pas le poids dans le cadre de la conformité des contrats peuvent quand même gérer la situation ?

BRUCE TONKIN: C'est une excellente question. C'est pour David, me semble-t-il, en termes de conformité des contrats, comment la mettre en œuvre.

DAVID CONRAD: Les responsabilités de mon groupe sont de collecter et de publier des faits non biaisés pour faciliter les discussions relatives aux politiques dans la communauté.

La conformité a accès à ces informations, comme tout le monde, et donc ces informations sont toujours rendues publiques, tant que nous le pouvons, sur la base des accords, etc.

Dans le cadre des données du DAAR, de toute évidence, ce que je vous ai montré sur le diagramme, les cercles rouges, donc 13 dans le rapport DAAR, identifient ou signalent que quelque chose d'étrange a lieu. Donc ceci fait partie de l'effort proactif que j'ai évoqué.

Donc dans le cadre d'un dialogue avec les bureaux d'enregistrement ou opérateurs de registre, nous essayons d'identifier quels sont les problèmes qui donnent lieu à ces comportements anormaux. Cela ne veut pas forcément dire qu'il y a un mauvais acteur, mais il y a quelque chose d'étrange qui est en cours. Et donc il faut essayer d'identifier ce qu'est cette situation étrange pour l'atténuer.

BRUCE TONKIN: Merci David. Nous allons maintenant passer aux gens qui ont la main levée.

Vous avez déjà essayé Jannett, donc je vais essayer de lui repasser la parole. Le micro est ouvert, si vous souhaitez poser votre question.

Bon… Je passe à la prochaine personne. Luisa Paez ? Posez votre question, allez-y. Non ? Très bien.

Je vais passer la parole à la dernière personne qui a levé la main. Kavouss Arasteh. Allez-y vous avez la parole, votre micro est ouvert. Ha ! ça ne marche toujours pas… Votre micro est ouvert, donc…

Ha, allez-y, nous vous entendons.

KAVOUSS ARASTEH: Oui, bonjour ou bonsoir. Une petite question. Quelle que soit l'exactitude des données relatives à l'utilisation malveillante du DNS, etc., quels sont les domaines dans lesquels nous n'avons pas encore

réussi à lutter contre cette utilisation malveillante, quelles sont les raisons de ces situations, et que pouvons-nous faire ?

Toutes les actions coordonnées et harmonisées au sein de l'ICANN, en ce qui concerne la lutte contre ces domaines, dans lesquels nous n'avons pas réussi m'intéressent. Quel est le plan coordonné que nous avons pour progresser dans ce domaine ?

BRUCE TONKIN: Merci Kavouss. Je crois qu'il y a plusieurs panélistes qui en ont parlé, cela partie de la transcription, mais est-ce que quelqu'un souhaite revenir sur ce qui fonctionne, ce que nous avons déjà fait ? Y a-t-il des panélistes qui souhaitent intervenir là-dessus ?

LAUREEN KAPIN : Oui, je souhaite remercier Kavouss pour sa question. Si on avait une réponse parfaite pour cette question très importante, et bien les choses seraient beaucoup plus claires pour l'avenir.

Mais j'aimerais quand même mentionner certaines des informations très utiles qui ont été mentionnées dans l'étude commanditée par l'équipe de révision CCT et qui donc a constaté plusieurs choses qui sont indiquées dans le chat également. Il semblerait qu'il y a une concentration de mauvais acteurs dans l'utilisation malveillante du DNS chez un nombre limité de bureaux d'enregistrement et d'opérateurs de registre. Et donc nous devons nous améliorer dans le domaine de l'identification et de la prévention d'une utilisation

malveillante systémique du DNS de la part de certains acteurs, des récidivistes pour ainsi dire. Ce serait un bon point de départ.

Et l'équipe de révision CCT a fait des recommandations tout à fait utiles dans ce domaine, en particulier sur le fait qu'on pourrait mettre en place un processus pour remettre en cause certains bureaux d'enregistrement ou opérateurs de registre qui, pour ainsi dire, sont des refuges pour ces mauvais acteurs. Il pourrait donc y avoir un processus qui leur permette d'expliquer pourquoi il y a des taux d'utilisation malveillante aussi élevés dans leur système, et pourquoi ils n'arrivent pas à s'occuper de cette situation.

Ce serait une petite étape qui pourrait être engagée.

BRUCE TONKIN: Merci beaucoup Laureen. Nous allons prendre une autre question de Susan Payne. Si on peut lire cela peut-être ?

RIA OTANES : Oui, Susan Payne : Laureen nous avons parlé dans le PDP [RPM] de ce concept d'interdiction de voler. Par exemple où l'on parle de perte du DRP, mais il y a des défis à relever pour mettre cela en place. Est-ce que vous avez une idée sur comment mettre cela en place ?

LAUREEN KAPIN : Oui, c'est en effet difficile, c'est une question difficile. Je crois que tout d'abord vous devez commencer avec des données. Vous devez vous

assurer que vous avez des informations sur les bureaux d'enregistrement qui soient les bonnes, qui soient précises, que vous n'avez pas d'informations fausses, d'alias et ainsi de suite.

Et également je crois qu'il faut avoir des normes sur ce quoi constitue une conduite néfaste ou négative. Donc par exemple, si vous avez un système, vous avez trois abus, au troisième là vous aurez des conséquences très sérieuses. Et bien, je crois que cela nous permettrait de mettre en place des bonnes données et des normes sur ce quoi constitue un comportement malveillant où une entité n'aurait plus le droit, le privilège, d'enregistrer des noms de domaine.

Ça, je crois que ce serait des mesures qui pourraient être prises en supposant que la communauté engagée dans le travail visant à s'assurer que nous avons de bonnes données et que nous avons des standards, des normes tout à fait raisonnables, et bien à ce moment-là, une fois qu'on a bien défini les comportements malveillants, et bien là je crois que ça pourrait fonctionner, c'est possible, c'est faisable, mais ça prendra du temps. Et une analyse et un débat analytique sur les données.

BRUCE TONKIN: Merci beaucoup Laureen. Nous avons une autre question je crois, une question anonyme ? De Fabricio ? Non ? Ou il y a une autre personne qui n'a pas donné son nom. On n'a parlé d'une approche avec des écrans de protection sur les données collectées, sur la précision des données, pourquoi ne pas avoir des mécanismes de sauvegarde un

petit peu différents, sur par exemple les personnes qui essaient d'enregistrer « trouver un remède à la Covid 19 », ce type de noms de domaine.

LAUREEN KAPIN : Je suis d'accord avec cela, avec cette suggestion. Il y a surement une possibilité à ce niveau, d'être proactif, et de prendre des mesures pour envisager les noms de domaine qui, dans leur nom, ont un message faux, un message erroné.

Et il y a des bureaux d'enregistrement qui ont fait ce travail, qui ont regardé de très près les enregistrements dans leur système, des enregistrements de noms de domaine qui les préoccupaient. Et je sais que c'est très difficile d'effectuer cela d'une manière très efficace sans avoir beaucoup de ressources. Donc a peut-être besoin de systèmes plus automatisés à ce niveau.

Mais je crois que c'est quelque chose qui pourra être mis en place dans la catégorie des écrans de protection, des boucliers, et de voir comment un message implicite, qui est trompeur, ne sera pas accepté, dès le départ par, par exemple, le bureau d'enregistrement.

BRUCE TONKIN: Merci beaucoup Laureen. Question pour Graeme d'une personne qui n'a pas donné son nom.

RIA OTANES : Pour Graeme : Et bien on a demandé à l'ICANN de travailler avec des bureaux d'enregistrement pour avoir un outil de validation, et la délégation croisée est tout à fait commune. On a vu qu'il y a beaucoup de ccTLD qui l'utilisent pour combattre les abus sur la Covid 19. Est-ce qu'on peut avoir des processus de validation croisée, et pourquoi on ne le fait pas plus fréquemment ?

GRAEME BUNTON : Merci de la question. Je ne sais pas si je serai en mesure de répondre à cette question.

La réponse la plus courte serait : c'est plus compliqué que vous ne le pensez. Nous avons des entreprises mondiales qui travaillent donc dans plusieurs pays et régions géographiques, et la validation croisée est très complexe. Et il y a des personnes qui utilisent différentes îles, qui sont peut-être au New Jersey, différents États. Donc je ne vais pas rentrer dans les détails, mais c'est difficile à effectuer, c'est très complexe.

BRUCE TONKIN: Oui, merci beaucoup. Est-ce que quelqu'un d'autre voudrait rebondir là-dessus ? Laureen, vous avez parlé de précisions et de l'importance de la précision en rapport avec l'identification des cas d'utilisation malveillante.

Non ?

MARY WONG: Oui, je crois qu'un de nos panélistes, Jim Galvin, voudrait rebondir.

BRUCE TONKIN: Oui, allez-y Jim, vous avez la possibilité de vous exprimer là-dessus.

JIM GALVIN: Oui, moi je réfléchissais à cette question, sur la précision des données dont on parlait tout à l'heure. Qu'est-ce qu'on a réussi, ou moins réussi, quels sont les défis à relever à l'avenir.

Moi, je crois qu'il y a deux points que j'aimerais soulever, deux défis à relever.

Lorsqu'on réfléchit à l'amélioration du système, je crois qu'il faut bien comprendre que nous n'avons pas un seul système pour faire respecter ces règles. Par exemple, pour les opérateurs de registre, nous avons les gTLD, nous avons les ccTLD, et les mécanismes ne sont pas les mêmes. Donc, est-ce que les standards de comportement pourraient être les mêmes dans ces deux domaines ? Non, il y a beaucoup de différences.

On en parle beaucoup. Ici, sur quoi pourrait-on nous concentrer ? Sur les gTLD, pour améliorer la situation des gTLD. Et lorsque l'on parle des ccTLD, on voit qu'il y a des règles de précision des données au niveau des ccTLD qui permettent de limiter certains abus. Mais ça c'est deux catégories différentes, et c'est bien cela le problème qu'il faut garder à l'esprit.

On cherche des normes de comportement, mais elles ne peuvent pas s'appliquer à toutes les catégories.

Lorsque l'on pense, également, au seuil à définir pour l'utilisation malveillante, lorsque l'on parle du système DAAR, lorsque l'on parle donc de l'aspect volontaire également, on n'a pas toutes les données à notre disposition. Donc la présence d'abus n'indique rien de plus que c'est l'endroit où cette personne a agi aujourd'hui, et il va peut-être faire une utilisation malveillante à un autre endroit du système demain. Donc parfois les données ne vont pas donner assez d'information.

Donc moi je crois qu'il faut garder cela à l'esprit lorsqu'on essaye de trouver des règles qui semblent être très contrastées. C'est plus difficile que cela, à la fois au niveau juridique et au niveau des normes que nous pourrions définir.

BRUCE TONKIN: Merci beaucoup.

Je crois que je vais essayer de résumer un petit peu la situation pour que nous puissions arrêter à l'heure.

J'aimerais tout d'abord remercier tous les intervenants qui ont décrit un petit peu leur travail et notamment lors de la pandémie de 19, ces derniers mois, qui ont apporté des suggestions sur la manière dont on peut reporter les abus, les utilisations malveillantes.

Je crois que Jeff a parlé du groupe sécurité et stabilité avec un ensemble d'outils, de processus, de comptes-rendus, de rapports possibles sur les abus et la gestion rapide de ces utilisations malveillantes, avec des meilleures pratiques qui peuvent être documentées. Les bureaux d'enregistrement, les registres, et les parties prenantes ont défini beaucoup plus l'utilisation malveillante, et ça c'est très utile.

Et nous avons entendu parler de la part de Brian au niveau des registres, les incitations que nous pourrions avoir pour un plus grand respect des règles, pour développer peut-être plus des systèmes et des processus.

Laureen a mentionné que ce qui a été très utile pour les forces de l'ordre, c'est d'avoir les bons contextes, et avoir la possibilité d'avoir une escalade des mesures de prises. Nous avons vu qu'un rapport entre les opérateurs de registre au niveau d'un pays et les forces de l'ordre peut être très utile ces mois derniers. S'ils se connaissent, et bien les forces de l'ordre pourront réagir plus rapidement, s'il y a une bonne communication. Il faut qu'il y ait les contacts possibles entre différents pays parfois.

Et Laureen nous a également parlé des incitations.

On a également mentionné qu'une des caractéristiques des tendances que nous notons, c'est pour avoir une analyse plus précise des problèmes, des informations associées avec une personne.

Et David a parlé également des données que l'ICANN collecte pour identifier les diverses tendances les plus marquantes dans le cadre de l'utilisation malveillante du DNS, et identifier pourquoi, le pourquoi des problèmes, et combattre ces différents comportements néfastes.

Donc je crois que tous les participants à la table ronde se sont concentrés sur ce que l'on peut faire à l'avenir, avec des mesures tangibles.

Je crois qu'il faut remercier tous les participants. On a eu jusqu'à 440 personnes qui ont participé à cette séance plénière. Beaucoup de personnes ont utilisé le chat pour beaucoup débattre de ce thème. Donc c'est tout à fait utile. Nous utilisons notre temps à ces activités virtuelles tout à fait intéressantes.

Donc nous allons clore cette séance, nous allons remercier tous les intervenants et les applaudir.

Merci beaucoup. Merci à toutes et à tous.

[FIN DE LA TRANSCRIPTION]