ICANN71 | Forum de politiques virtuel – Discussion du GAC sur l’atténuation de l’utilisation malveillante du DNS
Lundi 14 juin 2021 – 14h30 à 15h30 CEST

GULTEN TEPE : La séance va commencer, nous allons lancer l’enregistrement.

Bienvenue à la séance du GAC de l’ICANN71 consacrée à l’atténuation de l’utilisation malveillante du DNS le 14 juin 2021.

Nous n’allons pas faire d’appel aujourd’hui, mais les registres de présences seront disponibles parmi les procès verbaux du GAC. Je rappelle aux membres du GAC de bien vouloir indiquer leur présence en mettant à jour leur nom sur Zoom et en y ajoutant leur affiliation ou leur pays de provenance.

Si vous souhaitez poser une question ou faire commentaire, veuillez le taper dans le chat en bas de la fenêtre Zoom en ajoutant au début et à la fin de votre phrase le mot « Question » ou « Commentaire » pour que tous les participants puissent le voir.

Le service d’interprétation simultanée pour les séances du GAC est disponible dans les six langues de l’ONU et le portugais. Les participants peuvent sélectionner la langue dans laquelle ils souhaitent écouter ou parler en cliquant sur l’icône d’interprétation situé dans la barre d’outils de Zoom.

Votre microphone sera désactivé pendant toute la durée de la séance, à moins que vous soyez dans la file d’attente pour intervenir. Si vous

souhaitez parler, veuillez lever la main dans la salle Zoom. Lorsque vous prendrez la parole, dites votre nom pour les enregistrements et la langue dans laquelle vous allez parler si ce n'est pas l'anglais. Veuillez parler clairement et à une vitesse raisonnable pour permettre une interprétation exacte de vos propos. Finalement, rappelez-vous de bien vouloir mettre en muet tous vos autres dispositifs et notifications vocales.

Cette séance, comme toutes les autres activités de l'ICANN, est régie par les normes de conduite requises par l'ICANN. Pour référence, vous trouverez le lien vers cette politique sur le chat.

Maintenant, je vais donner la parole à la présidente du GAC, Manal Ismail. Manal, à vous.

PRÉSIDENTE MANAL ISMAIL : Merci beaucoup Gulten et rebienvenue à tous à cette séance de 90 minutes au cours de laquelle nous allons aborder l'atténuation de l'utilisation malveillante du DNS. Nous espérons pouvoir finir d'ici 60 minutes et si nous pouvons accomplir cette tâche en l'espace d'une heure, nous allons commencer à travailler sur la rédaction du communiqué pour voir quels devraient être les messages clés à transmettre, les contenus et autres que devrait contenir notre communiqué.

Je vois déjà une liste d'intervenants du côté du groupe de travail sur la sécurité publique, et nos collègues japonais ont également invité des orateurs des groupes de travail anti-rançon logiciel et autres. Donc

sans tarder, je vais tout de suite céder la parole à… Qui va commencer ? Laureen ? Laureen, allez-y.

LAUREEN KAPIN : Bonjour à tous et bienvenue. Je m'appelle Laureen Kapin, je suis l'une des coprésidentes du groupe de travail sur la sécurité publique et je serai accompagnée de mon coprésident Chris Lewis-Evans et de mon collègue du bureau américain du FBI Gabe Andrews qui s'est levé de très bonne heure pour être là comme bien d'autres personnes. Nous avons des orateurs très spéciaux pour ce sujet. Nous avons notre collègue du Japon Shinya Tahata et les orateurs invités qui nous parleront d'une étude très récente au sujet de l'accès aux données d'enregistrement de noms de domaine.

Pour ce qui est des attentes que vous pourrez vous faire, vous voyez Manal que nous avons une liste assez pleine et je m'excuse dès maintenant si nous prenons plus que les 90 minutes qui étaient prévues pour cette séance. Nous nous efforcerons d'y parvenir, bien sûr. Et j'encourage tout le monde à bien vouloir se borner au temps qui leur est imparti. Nous allons réserver les questions pour la fin, à l'exception du collègue du Japon et des collègues qui ont fait l'étude qui, bien sûr, pourront répondre à des questions tout de suite à la fin de leur présentation s'ils le souhaitent.

L'utilisation malveillante du DNS est l'un des sujets récurrents au GAC étant donné son importance et vu qu'il s'agit également d'un sujet qui est en vogue en ce moment puisque l'infrastructure essentielle des finances et des systèmes industriels fonctionne sur internet et que

cela a un impact sur la vie des personnes au quotidien qui peuvent avoir de l'argent qui leur est volée et leur identité qui leur soit usurpée ou autre et qui utilisent, bref, le DNS pour pouvoir utiliser internet. Les délinquants par contre utilisent le DNS pour perpétrer ces attaques.

Voilà pourquoi nous revenons toujours sur le sujet de l'utilisation malveillante du DNS et nous avons différentes mesures que nous pouvons prendre en tant que communauté pour atténuer ce problème. Il existe un document du SSAC qui contient des propositions très concrètes. Notre collègue Gabe du FBI nous parlera du travail en collaboration avec les collègues des unités constitutives des parties contractantes sur des questions qui sont d'importance sur les réseaux zombie par exemple, les rançons logiciel et autres. On parlera du temps qui est nécessaire pour répondre aux demandes de données d'enregistrement. Comme vous le savez, ces informations peuvent être essentielles pour une enquête policière lorsque le DNS est exploité à des fins malveillantes.

Nous allons également parler de l'équipe de révision de la confiance, la concurrence et le choix du consommateur qui vise à garantir qu'il y ait des données qui soient disponibles au public pour tous ceux qui veulent savoir qui est le titulaire d'un nom de domaine pour qu'ils puissent arriver au bon endroit et pas à un lien où on voit des informations sur certains qui ne connaissent même pas la personne titulaire du nom de domaine.

Puis, nous avons une très bonne présentation des collègues d'en dehors de notre groupe. Le collègue japonais nous donnera une mise

à jour sur la conformité contractuelle qui est une mesure clé pour atténuer l'utilisation malveillante du DNS et sur les étapes à suivre, bien sûr. Nous avons tout un menu de sujets à aborder.

Je vais passer le bâton directement à mon collègue Chris Lewis-Evans du Royaume-Uni. Je vais sauter cette diapositive qui présente l'ordre du jour pour la séance d'aujourd'hui. Vous avez déjà toutes les informations sur les événements qui sont à venir sur le site de l'ICANN. Vous avez tout reçu, pas la peine d'entrer dans les détails. Chris, présentez-nous le SSAC s'il vous plaît.

CHRIS LEWIS-EVANS : Merci Laureen. Je vais très rapidement parler du document du SSAC qui présente une approche interopérable pour l'atténuation de l'utilisation malveillante du DNS. Il s'agit d'un cadre proposé qui couvre toute la documentation.

Certaines des informations qui apparaissent ici sont d'intérêt pour nous au sein du PSWG et du côté des politiques publiques de ce point de vue. Et le premier est la disponibilité et la qualité des informations de contact.

En général, les agences d'application de la loi ont plus de mal à pouvoir trouver des résolutions pour les cas d'utilisation malveillante du DNS et c'est le cas également dans l'industrie, ce qui fait qu'au lieu de se rendre au bon endroit avec la bonne approche pour résoudre ces problèmes, on finit par envoyer des avis d'utilisation malveillante un peu partout jusqu'à ce que l'un de ces avis génère l'effet escompté. Il

faudrait donc qu'il y ait un seul point de contact qui serait alors responsable de vérifier quel serait le point de contact correct avec qui échanger.

Puis, nous avons les voies de délégation qu'on fait suivre aux cas. Lorsqu'on n'est pas en lien direct avec l'entité qui est responsable et à l'origine de cette utilisation malveillante, on peut ne pas avoir de réponse. Alors à travers ces trajets, on voit comment adresser la responsabilité et comment faire en sorte que la demande soit transmise et appliquée.

Il existe bien sûr des lignes chronologiques plus efficaces que d'autres. Et certains membres étaient en désaccord avec les propositions du document SSAC115. Mais à travers les processus d'escalade, on a vu que cela pouvait prendre 24 heures de passer d'un acteur au suivant, donc pour chaque escalade – et je voulais le dire. Mais au moins, c'est un départ meilleur que ce que l'on pourrait avoir à présent.

Les agences d'application de la loi en général sont très favorables à faire en sorte qu'il y ait des normes d'évidence et une terminologie. Je pense que cela est tout à fait positif. Cela peut s'appliquer aux différents niveaux des personnes qui sont impliquées et qui sont responsables de gérer les réclamations d'utilisation malveillante du DNS et cela pourrait réduire la charge de travail sur les entités qui doivent répondre aux requêtes.

On a également des délais raisonnables pour passer à l'action. C'est en lien avec les processus d'escalade, bien sûr. On n'a pas des délais

raisonnables pour l'instant et il faudrait améliorer la manière d'escalader les cas.

Et finalement, il y a la disponibilité et la qualité des informations de contact qui sont liées avec beaucoup des autres points. C'est une interdépendance importante. Pour pouvoir avoir le résultat souhaité, il faut avoir les bonnes informations de contact qui sont parfois difficiles à trouver. Il faut passer par des revendeurs ou autres. Puis, on a également les données d'un répertoire de recherche RDS qui vous empêche de prendre les mesures les plus raisonnables et appropriées.

Voilà pourquoi le PSWG s'est surtout concentré sur tout ce qui est proposé ici bien sûr, mais le principal, ce sont les points de contact et les processus d'escalade. Diapositive suivante.

Dans le document SSAC115, à travers ses différentes recommandations, on considère en un peu plus de détails le fait que l'utilisation malveillante du DNS n'est pas circonscrite à la communauté de l'ICANN. On voit alors comment l'ICANN pourrait entamer une conversation et mettre en œuvre les meilleures pratiques au sein de l'industrie sachant qu'il y a beaucoup plus d'acteurs que ceux qui sont impliqués à l'ICANN. Comme je l'ai déjà dit, la proposition préférée du PSWG est celle d'avoir un facilitateur ou un responsable du signalement l'utilisation malveillante commune. Cette personne est responsable d'engager cette conversation et de voir comment faire en sorte que les bonnes mesures puissent être mises en œuvre. Nous avons déjà discuté avec différentes parties et il s'agit effectivement de quelque chose que je voudrais voir mis en œuvre à

titre personnel. Mais je pense que du point de vue du GAC, nous pouvons également appuyer cette proposition et y apporter des contributions et des informations pour voir comment cela pourrait fonctionner dans chacune de nos juridictions.

Je sais qu'il y a beaucoup d'autres sujets à aborder alors sur ce, je vais céder la parole à Gabe, qui va nous parler des cadres de DGA.

GABRIEL ANDREWS : Merci Chris et bonjour. Je vais consacrer 10 minutes à parler de l'algorithme de génération de domaines et du cadre qui est utilisé. Il s'agit d'un projet qui était un effort conjoint entre le groupe de travail des représentants des opérateurs de registre et celui de la sécurité publique. Je prendrai une dizaine de minutes et je vais demander que l'on donne également la parole à James Galvin de Donuts pour parler de ce sujet.

Pour définir de quoi je parle, je parlais de DGA tout à l'heure ; il s'agit de quelque chose de technique mais qui est lié aux réseaux zombies. Ce sont des réseaux de dispositifs compromis qui sont contrôlés par des délinquants. Et certains des réseaux zombies les plus grands et les plus dangereux qu'on a dû gérer par le passé sont Avalanche et Configure qui étaient contrôlés par les personnes malveillantes qui contrôlaient à travers l'utilisation de l'algorithme de génération de domaines ces réseaux zombies. Ces algorithmes de génération de domaines peuvent être utilisés comme informations d'entrée à l'avenir qui génèrent un algorithme spécifique à cette date et à ce moment. En général, c'est comme si on avant des drôles de problème,

mais ce n'est pas cela, le problème ; il s'agit d'attaques que nous ne voyons pas très fréquemment mais qui ont un impact très profond.

Alors lorsqu'on agit contre la grande quantité de domaines qui sont associés aux réseaux zombies et qui utilisent les DGA, c'est rare comme je le disais mais cela a un grand impact sur les forces d'application de la loi et sur les mesures que nous prenons. Donc s'il y a des centaines de milliers de noms de domaine qui sont en lien avec le DGA qui sont générés chaque année, les agences d'application de la loi doivent saisir les tribunaux du cas pour pouvoir faire en sorte que ces DGA soient modifiés, et cela pourrait se faire d'année en année.

De la même manière, les registres préfèrent ne pas devoir avoir recours à l'ICANN pour que des actions soient mises en œuvre et pour que les forces de l'ordre puissent répondre. Dans ce cadre, nous avons voulu créer un processus qui permette d'avoir un point unique pour les registres grâce auxquels on puisse mettre en œuvre des actions qui soient permanentes. Ce type de solution pourrait répondre aux besoins de répondre à ces problèmes et ne pas avoir à refaire le processus auprès de l'ICANN à chaque fois qu'un problème comme cela se présente. Donc le groupe de travail sur les abus des parties prenantes a été très utile, il a beaucoup travaillé pour établir ce processus afin que toutes les parties concernées, registres, forces de l'ordre, etc. puissent prendre des mesures responsables afin de lutter contre ce type d'abus.

Ceci dit, je vais maintenant demander à Jim Galvin de prendre la parole au nom du groupe des représentants de registres pour voir s'il souhaite prendre la parole.

JIM GALVIN : Merci beaucoup.

Il manquerait une dernière diapositive. Le cadre concernant l'abus du DNS, c'est une autre diapositive à laquelle je fais référence. Merci beaucoup, oui, c'est celle-là.

Le cadre sur l'utilisation malveillante du DNS est un cadre général très important qui est en lien avec le SSAC115 dont a parlé mon collègue et qui parle du grand écosystème auquel fait référence le SSAC115. Et vous voyez à droite les titulaires de nom et les registres, mais ils ne sont qu'une petite partie de l'écosystème sur lequel nous pouvons agir.

Ce cadre contient une définition de ce qu'est l'utilisation malveillante du DNS et établit ce que les registres et bureaux d'enregistrement peuvent faire dans ce contexte. Le résultat, c'est que nous avons un ensemble de solutions qui peuvent être mises en place dans cet espace avec une certaine marge dans laquelle nous pouvons agir de manière rapide.

Comme il y est dit dans le SSAC115, ce cadre qui a été établi il y a quelques années a été adopté par un certain nombre de parties contractantes et a été reconnu de manière officielle par les deux

groupes de représentants de registres et de bureaux d'enregistrement, sachant qu'il y a beaucoup d'autres acteurs dans cet écosystème.

À l'instar de ce qui s'est passé avec le SSAC115, nous avons établi des calendriers d'action dans le cadre de cet écosystème pour tous les acteurs concernés. Le point important est de comprendre que le problème dépasse ce que nous pouvons faire dans notre espace limité et c'est pour cela qu'il y a un besoin d'un facilitateur commun auquel fait référence le SSAC115 et qui va au-delà des bureaux d'enregistrement et des opérateurs de registre. Donc ce facilitateur a un rôle à jouer dans ce système.

Ensuite, un grand nombre des actions et un grand nombre des calendriers qui sont établis dans le cadre du SSAC115 sont établis parce que cela dépend du fait que vous avez recours à la bonne personne au bon moment. Dans un nombre limité de circonstances, en tant que bureaux d'enregistrement, vous devez vous adresser aux bonnes parties, aux parties concernées. Mais parfois, il est beaucoup plus facile de s'adresser directement à la personne ou à la partie qui peut mieux être à même d'agir sur le problème concerné. C'est pour cela qu'il est tellement important de pouvoir s'adresser au bon acteur, à la bonne partie prenante.

Dans le cadre du groupe de travail CPWG, nous avons travaillé directement avec le PWSG également. Le DGA est un exemple du travail que nous avons fait. Nous avons bien travaillé avec eux et avec l'ICANN pour créer un cadre volontaire pour tous ceux qui participent activement à ce type d'activités de lutte contre l'utilisation

malveillante du DNS et pour essayer d'endiguer le problème de l'utilisation malveillante du DNS.

Merci beaucoup.

GABRIEL ANDREWS : Merci beaucoup. Je voulais juste mettre l'accent sur le fait que nous sommes toujours ouverts à davantage de coopération de la part d'autres acteurs, donc nous invitons les personnes intéressées, les différentes unités constitutives, les membres du GAC ainsi que les forces de l'ordre à prendre part à ce travail qui est fait dans le cadre de notre travail, parce qu'il y a toujours des progrès à faire. Merci beaucoup de votre attention et de votre temps.

LAUREEN KAPIN : Merci James, merci Gabe de cette présentation.

Nous allons changer de sujet maintenant et nous allons passer à un sujet qui a été abordé brièvement tout à l'heure, le SSAC115 pour ce qui est des requêtes d'information dans le cadre du WHOIS. C'est un sujet qui a fait l'objet de très longs débats au sein de la piste de travail 1 de l'équipe de mise en œuvre.

Pour vous donner un petit peu de contexte, les requêtes urgentes sont très limitées au niveau des scénarios possibles. Elles sont limitées à certaines circonstances qui peuvent supposer une menace imminente à la vie, des blessures graves ou des problèmes avec l'infrastructure critique ou l'exploitation des enfants dans des cas où la divulgation de

ces données est nécessaire pour combattre ou donner une solution à ces menaces. Il s'agit de scénarios qui sont rares.

Les représentants du GAC dans l'équipe IRT ont voulu que le délai pour répondre à ce type de question soit de 24 heures. Cela contraste avec le délai actuel qui est de 30 jours.

Il a été envisagé que le délai pour ces requêtes urgentes soit établi par l'équipe de travail. Nous voulions donc attirer votre attention sur cela parce que le débat qui est en cours parle d'un délai de 24 heures versus un délai que les forces de l'ordre et les experts de la protection des consommateurs considèrent trop long. Donc la discussion est en cours et il y a un argument qui plaide pour un délai de 3 jours ouvrables. Mais lorsque nous allons au-delà des 24 heures et que l'on parle de jours ouvrables, on peut avoir des situations où quelque chose de très mauvais se passe, pendant le weekend par exemple. Si vous vous en tenez à trois jours ouvrables et qu'il y a des vacances ou un weekend au milieu, vous pouvez vous retrouver dans une situation où une requête vraiment importante et vraiment urgente –parce qu'elle implique des blessures ou des dommages à des infrastructures critiques – n'aura pas de réponse. C'est pour cela qu'il faut se pencher sur la question du délai pour cette catégorie de requêtes rares certes, mais qui requièrent une réponse très rapide. Diapositive suivante s'il vous plaît.

Il s'agit d'une question qui est en lien avec les données d'enregistrement et qui est très importante pour lutter contre l'utilisation malveillante du DNS. Cela est en lien avec la diapositive

qu'a montrée James quand il a parlé des acteurs clés de l'écosystème, parce qu'il y a les bureaux d'enregistrement, les opérateurs de registre, mais il y a une troisième catégorie, soit les revendeurs. Donc dans le cadre de la révision CCT, il y a eu la recommandation 17 qui cherchait à dire que même si les bureaux d'enregistrement publient les données d'enregistrement et que l'on peut y accéder pour avoir ces informations, parfois, ce n'est pas le bureau d'enregistrement qui a l'information mais une partie contractante comme un revendeur. Donc c'est pour cela que l'équipe a fait une recommandation, à savoir que l'ICANN collecte des données et qu'elle rende publique la chaîne d'enregistrement. Et le Conseil d'Administration a accepté cette recommandation et il a indiqué qu'elle soit mise en place.

Le problème ici, c'est que même si parfois ces informations se trouvent dans les fichiers publics d'enregistrement de noms, elles ne sont pas obligatoires. Et j'ai tenu à attirer votre attention sur cette question parce qu'il faut encore travailler là-dessus pour que cette recommandation soit complètement acceptable et pour qu'elle soit mise en œuvre. Pour que le Conseil d'Administration accepte la mise en œuvre complète de cette recommandation, il faudrait que l'on puisse accéder à la chaîne complète d'enregistrement. Pourquoi c'est important ? Parce que les forces de l'ordre peuvent gagner du temps car elles accèdent ou s'adressent directement à la partie concernée et non à une partie qui à son tour va conduire à une autre partie et ainsi de suite. Nous pensons que c'est une solution rapide qui ferait gagner énormément de temps aux forces de l'ordre et aux agences de protection des consommateurs. Diapositive suivante s'il vous plaît.

Ici, nous allons passer à une présentation qui aborde la question de l'accès aux données d'enregistrement. Elle va porter sur une étude récente faite par le groupe de travail anti-abus pour la messagerie, les logiciels malveillants et les mobiles, le groupe de travail M3AA. Donc les représentants de ce groupe vont vous en parler davantage. Pour vous donner un petit aperçu, il s'agit d'une enquête qu'ont menée les enquêteurs en matière de cybercriminalité pour essayer de comprendre comment l'application du RGPD par l'ICANN a eu un impact sur l'information au WHOIS et la disponibilité de ces informations et dans quelle mesure les spécifications temporaires ont eu un impact sur l'utilisation de ces données d'enregistrement. Comme nous l'avons dit, le WHOIS est un outil très important pour les enquêtes des forces de l'ordre et pour les initiatives de lutte contre les abus.

Je vais donc maintenant passer la parole à ma collègue et je les remercie d'avance de cette présentation. Merci Laurin.

LAURIN WEISSINGER : Je vois déjà ma présentation à l'écran, merci. Passons à la disponible suivante s'il vous plaît. Voici le sondage dont parlait Laureen qui a été réalisé par l'APWG et le groupe de travail MAA. Et les personnes qui sont à l'écran sont les principaux chercheurs : moi-même, Dave Piscitello que connaissent déjà bon nombre des participants ici et Bill Wilson qui vous adressera la parole par la suite, qui est conseiller sénior au MAAWG. Diapositive suivante.

Pour que tout le monde soit au courant de ce qu'est le MAAWG, en fait, le MAAWG a été fondé en 2004. Il s'agit du groupe de travail anti-abus mobiles, rançons logiciel et messagerie. Ils travaillent avec la communauté en ligne pour trouver l'abus en ligne et l'exploitation des données des utilisateurs.

Le MAAWG, le groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles, publie des documents sur les meilleures pratiques, des déclarations de position et autres pour aider la communauté à lutter contre l'utilisation malveillante, mais il fait également le plaidoyer de la politique publique, pas le lobby, mais à travers le fourniture de directives techniques et opérationnelles pour les gouvernements et pour les agences de politique publique de gouvernance de l'internet. Diapositive suivante.

Pour cette étude, nous avons reçu 277 réponses. Nous avons envoyé des demandes de réponse à l'enquête à des listes d'emails spécifiques et à des contacts spécifiques, ce qui fait que les répondeurs viennent de l'environnement de la cybersécurité, de l'application de la loi, de la sécurité publique, etc. ; il s'agit d'un groupe très spécifique. Il faut dire ici que le WHOIS est utilisé à des fins très diverses ; notre étude portait également sur cela. Donc l'idée est de voir combien de registres sont accédés à un moment donné, à ce qui se passe avec ces registres, comment ils pourraient être plus utiles, quelles sont les données qui sont demandées. Il y a de grandes différences entre les analyses de données qui se font en vrac et qui demandent beaucoup de données très fréquemment et les enquêteurs qui demandent de registres, ce qui n'est pas fréquent et qui se fait manuellement.

GULTEN TEPE : Laurin, je vais vous demander de bien vouloir parler un peu plus doucement, d'accord ?

LAURIN WEISSINGER : Oui, bien sûr.

Voyant ici les répondants. La plupart viennent du secteur de la cybersécurité : on a 40 % de professionnels de ce secteur, 25,4 % de professionnels du secteur de la propriété intellectuelle et juridique, mais il y a également des répondants du secteur académique, commercial, de l'hébergement, des FSI et des forces de l'ordre et de la sécurité publique.

Nous avons comparé nos résultats actuels et la composition actuelle avec ceux de l'étude de 2018 et nous avons beaucoup renforcé la participation du secteur juridique cette fois-ci.

Il est important de signaler que même dans cet échantillon très particulier, parce qu'il n'y a pas beaucoup de personnes intéressées par cela, seul 1 répondant sur 10 envoie plus de 10 000 requêtes par jours. Plus du deux-tiers des répondants envoient moins de 100 requêtes quotidiennes. Et bien sûr, le principal de notre étude n'était pas tout simplement de savoir quels étaient ces chiffres mais comment sont utilisées les requêtes et à quelle fin.

On a ici l'utilisation combinée entre 2018 et 2021 et nous voyons à travers les données consolidées ici qu'il y a eu une réduction dans le

volume de requête, seules quelques augmentations. Il y a également eu des usages qui ne sont plus fréquents mais des données techniques, c'est-à-dire des éléments qui ne sont pas expurgés en 2021 et qui correspondent aux mêmes requêtes, c'est-à-dire plus de 50 % des répondants disent que le volume n'a pas changé.

L'accès au WHOIS est reflété dans les chiffres comme je le disais tout à l'heure et vous voyez que 36 % utilisent des requêtes web sur le WHOIS. Les autres utilisent des technologies variées.

Il y a beaucoup plus sur ces informations particulières sur le RDAP sur le rapport que je vous invite à lire. Ici, vous n'avez qu'une petite présentation. D'après nos répondants, l'effet de la spécification temporaire, le temps d'atténuation de ces problèmes dépasse largement les seuils acceptables – c'est ce qu'ont répondu la plupart.

Comme vous le voyez, moins de 10 % disent que les enquêtes ne sont pas affectées et un peu plus de 20 % disent : « Oui, cela a un impact sur nous mais nous pouvons toutefois compléter notre travail dans des délais acceptables. » Diapositive suivante.

Et si nous comparons cela aux données de 2018, vous verrez qu'il y a une petite hausse du côté des personnes qui disent que le temps d'atténuation dépasse le seuil acceptable de 65 % à 70 %, donc c'est empiré légèrement. Diapositive suivante.

Comme vous voyez et cela est surprenant, plus de 80 % nous disent que le temps de répondre aux activités malveillantes en ligne a augmenté et que le temps de répondre aux domaines malveillants a

également augmenté. Il faut donc garder à l'esprit qu'au cours des premières heures, le premier jour ou deux, il est nécessaire d'agir et de lutter contre les activités criminelles pour pouvoir en faire quelque chose, pour pouvoir en profiter. Il faut agir le plus vite pour pouvoir prendre des mesures véritablement efficaces.

Pour une synthèse des sujets du rapport, vous pourrez aller lire le rapport si cela vous intéresse. Il y a beaucoup de questions qui n'ont pas été présentées ici ou pas en détail. Seul un quart des répondants ont pu trouver des sources de données alternatives d'après ce qu'ils ont manifesté. Ils ont déjà des données préalables du système du WHOIS. L'attribution est très affectée, ce qui n'est point surprenant. Et 9 sur 10 répondants manifestent avoir des problèmes au cours du moment de l'attribution en raison de l'expurgation des données. Plus de 50 % considèrent l'expurgation des données des personnes juridiques et des personnes en dehors de l'Union européenne comme étant excessive et seuls 2,2 % considèrent que la spécification temporaire fonctionne. Diapositive suivante.

Alors l'une des manières que nous avons de traiter les données expurgées du WHOIS est d'envoyer des demandes pour pouvoir accéder aux données qui sont expurgées ; 34,4 % des répondants nous disent qu'ils considèrent cela un peu trop compliqué, plus d'un quatre disaient qu'il faut le faire et le reste, comme vous voyez, est divisé. Il y en a pas mal qui ne savaient même pas que cela était disponible et ne savaient pas comment l'utiliser. Il y a également le groupe qui ne s'y intéresse pas, qui n'envoie pas de requêtes, qui ne voit pas cela comme une partie des cas d'utilisation.

Ici, nous voyons encore une fois lorsque nous comparons les réponses à celles de 2018 que les temps de réponse ont en moyenne augmentés et en particulier – et cela est intéressant – plus d'une semaine, plus de sept jours, ce qui fait que la moyenne de temps de réponse est d'une semaine puisque 36 % disent cela. En 2021, cela prend plus de sept jours à 60 % et ce n'était que 36,1 % en 2018, donc on a beaucoup dépassé les délais qu'on avait à l'époque.

Ce cadre de 30 jours est-il acceptable pour les répondants pour pouvoir obtenir la divulgation des données ? La réponse est non, on ne peut pas attendre 30 jours pour se voir accorder l'accès aux données. Les chercheurs à 50 % disent : « Oui, ce serait bon. » Dans le secteur des marques commerciales, ce serait correct peut-être, mais tous les autres ont besoin de beaucoup plus de rapidité.

On a ici la possibilité des 10 jours. On demande si c'est acceptable et ce n'est toujours pas considéré acceptable par les répondants. Encore une fois, il y a beaucoup plus de personnes qui pourraient être contentes avec ces résultats de 10 jours ; c'est un peu partagé.

Ici, vous voyez ce qui serait considéré correct par les répondants. Comme vous voyez du côté du malware, du phishing, de l'utilisation malveillante des rançons logiciels, du pourriel, pour le pourriel/spam, c'est moins de 4 ; pour les problèmes associés à la propriété intellectuelle, entre 5 et 6. Les chercheurs seraient satisfaits avec des délais de réponse de 10 jours.

Avec la divulgation, nous nous sommes concentrés sur les délais, mais nous devons également garantir que les réponses soient différentes.

Beaucoup sont ignorées, parfois ils sont reconnus et on reçoit un accusé de réception mais pas de réponse, les requêtes ne sont peut-être pas susceptibles d'être mises en œuvre et autres problèmes.

L'ICANN discute de systèmes de divulgation futurs en ce moment. Cela date d'il y a quelques mois, ce n'est peut-être plus d'actualité aujourd'hui. On parlait d'une approche qui soit mise en œuvre à travers un système payant, on disait qu'il n'y avait ni la capacité ni les ressources pour payer. 61 % des répondants disaient qu'ils n'étaient pas en mesure de payer des frais mais après, 39 % disent qu'ils peuvent les payer, 78 % pourraient payer des frais d'accréditation raisonnables et 61 % accepteraient des systèmes de tarification par volume ou au niveau. Et il y a des personnes qui ne sont point d'accord avec l'idée de devoir payer pour accéder à ces données. Diapositive suivante.

Finalement, de mon côté, je conclus avec cela, quel est votre niveau de satisfaction vis-à-vis des plaintes liées à la divulgation de données et à la conformité de l'ICANN avec l'accès des données d'enregistrement et les réponses aux requêtes ? On voit que cette image n'est pas très positive : 41 % des répondants étant très insatisfaits et 35,9 % disant être quelque peu insatisfaits.

Je vais maintenant céder la parole à Bill Wilson qui va faire une synthèse cette présentation. Diapositive suivante, merci.

BILL WILSON : Bonjour à tous. J'espère que vous m'entendez bien.

Il y a quatre remarques dont nous prenons note à partir de cela. Je pense que tout le monde est d'accord sur le fait qu'il nous faut avoir toutes les données liées possibles tout en protégeant la vie privée des personnes physiques. Les réponses à l'enquête indiquent par ailleurs que ce qui est discuté à l'heure actuelle à l'ICANN ne répondra pas aux besoins des agences d'application de la loi et des acteurs de la cybersécurité.

Troisièmement, l'ICANN doit établir un système fonctionnel d'accès aux données des titulaires de nom de domaine pour les parties accréditées et que ce système doit pouvoir être utilisé par les professionnels de la cybersécurité et par les agences d'application de la loi. Mais comme tel, cela doit fonctionner d'une manière qui élimine des délais et la charge et les coûts administratifs. Et cela devrait également inclure des contrôles de sécurité et de vie privée qui soient stricts. Il doit également y avoir une forme de responsabilité pour pouvoir maintenir le système en fonctionnement. Et quatrièmement, comme cela a été dit par Laurin, il y a deux types d'utilisateurs : on a les utilisateurs qui demandent beaucoup de volume, qui l'utilisent beaucoup, et les petits utilisateurs qui n'envoient des requêtes que de temps en temps, qui utilisent un volume plus petit. Le système doit pouvoir traiter les deux types d'utilisateurs. Diapositive suivante.

Les quatre principaux points que je voulais soulever ici sont les suivants. Les spécifications temporaires se sont avérées augmenter le temps requis pour pouvoir accéder à ces informations. L'accès opportun à ces informations représente un véritable enjeu.

Et ensuite, le système n'est pas uniforme pour tous le bureaux d'enregistrement. Chaque bureau d'enregistrement a ses propres spécificités et cela représente des obstacles pour les investigateurs.

Le système de requête formel pour pouvoir accéder à des données expurgées est souvent en panne. Il y a des requêtes qui ne sont pas prises en compte, qui sont refusées ou auxquelles on ne répond simplement pas. Donc il n'y a plus de valeur à ce système.

Ensuite, pour ce qui est des processus de conformité contractuelle de l'ICANN, ils sont décrits comme étant trop longs, comme n'étant pas suffisamment efficaces et comme ne pouvant pas répondre aux demandes ou n'étant pas capables de résoudre le problème.

Si vous avez des questions, n'hésitez pas à nous écrire à publicpolicy-chair@mailman.maawg.org et nous allons essayer de faire notre mieux pour y répondre. Merci beaucoup.

LAUREEN KAPIN : Merci beaucoup à tous les deux pour ces deux présentations très intéressantes et très concrètes car elles nous a montré des exemples concrets d'utilisateurs, d'investigateurs, de personnes qui travaillent dans le domaine de la cybersécurité. Donc nous avons beaucoup d'éléments pour réfléchir, pour essayer de faire en sorte que le système fonctionne de manière appropriée et équilibrée afin que les données puissent être protégées mais que l'intérêt public soit préservé.

Nous allons maintenant passer à un sujet complètement différent qui sera présenté par notre collègue du Japon, Shinya Tahata. Je vais donc lui donner la parole.

SHINYA TAHATA : Merci beaucoup Laureen.

Tout d'abord, j'aimerais exprimer ma reconnaissance aux coprésidents du groupe de travail de m'avoir donné cette opportunité de parler. Nous avons quelques informations à partager avec vous. C'est pour cela que je voudrais faire un aperçu des idées que l'on a débattues ainsi que des propositions concrètes à mettre en place.

À la réunion ICANN70, nous avons pu remarquer qu'il y avait encore des cas contre le RAA, par exemple il y avait certains bureaux d'enregistrement qui ne demandaient pas les informations exactes de la part des titulaires de nom et certains titulaires de nom ne suivaient pas les règles de l'ICANN et tout cela, malgré le fait de savoir qu'il est très important de pouvoir compter sur des informations WHOIS précises et exactes.

À partir des rapports CCT et d'autres travaux qui ont été faits, nous savons qu'il y a des informations précises qui sont demandées. Par exemple d'après l'équipe d'études, il y a plus de 15 domaines qui avaient été enregistrés par un seul titulaire de nom et cela, sans donner les informations qui sont requises dans le cadre du RAA. Il s'agit donc de sociétés qui ne sont pas conformes.

Et ici, je voudrais soulever trois points. D'un côté, la conformité. Il est important de collecter des informations exactes de la part des titulaires de nom au moment de l'enregistrement. Selon le RAA, les bureaux d'enregistrement doivent demander aux titulaires de nom des informations précises tel que le numéro de téléphone, l'adresse postale. Et la plupart des bureaux d'enregistrement suivent les règles de l'ICANN. Or, il y en a certains qui ne suivent pas ces règles et cela peut donner lieu à des abus du DNS. C'est pour cela qu'il est important de pouvoir corriger ces lacunes par la conformité contractuelle.

Deuxièmement, il est important de pouvoir vérifier l'identité des titulaires de nom. Dans le cadre du RAA, les bureaux d'enregistrement doivent prendre des mesures strictes, y compris la suspension du nom de domaine si les données du WHOIS ne sont pas correctes dans un délai de 15 jours. Et dans certains cas, ces données ne sont pas correctes. C'est pour cela qu'il faut suspendre les noms de domaine qui ne se conforment pas à cette disposition du contrat.

Ensuite, pour pouvoir vérifier ces informations, ces identités, il est important de pouvoir compter sur ces informations et de pouvoir confirmer que les bureaux d'enregistrement ont accès aux points d'accès de réponse à des abus. Il est important également de demander des preuves pour savoir si les noms de domaine ne s'adonnent pas à des activités malveillantes.

Ensuite, dans le SSAC115, on établit que des normes doivent être mises en place, y compris pour atténuer l'abus du DNS et mettre en application les dispositions des contrats. Donc je pense que ces trois

points nous permettent de continuer le débat par rapport à cette question afin de pouvoir mettre en place des mesures appropriées et répondre de manière efficace aux cas d'utilisation malveillante du DNS et pour pouvoir également vérifier l'identité des titulaires de nom. Nous pouvons donc partager nos conclusions à cette réunion avec les membres du GAC.

Merci beaucoup.

LAUREEN KAPIN : Merci beaucoup Shinya d'avoir partagé ces propositions très concrètes. Nous avons certainement un éventail de volets concernant l'utilisation malveillante du DNS auxquels il faudra réfléchir.

Maintenant, nous allons parler des mesures à suivre et finalement, nous allons réserver un petit créneau pour des questions et réponses. Ensuite, nous allons entendre une présentation qui fait référence aux dispositions contractuelles qui font référence à l'utilisation malveillante du DNS. Si vous voyez cette diapositive sur l'écran, elle fait référence à ce dont nous a parlé notre collègue du Japon.

Quelles sont les prochaines étapes ? Il y a eu beaucoup de propositions pour atténuer l'utilisation malveillante du DNS dans le cadre des procédures ultérieures de nouveaux gTLD, mais le groupe de travail PDP sur des séries ultérieures indiquait que l'utilisation malveillante du DNS devrait être traitée mais par rapport à tous les TLD et non seulement par rapport aux TLD génériques. Il s'agit donc d'une approche qui devrait être holistique selon la GNSO.

Pour la première série de nouveaux gTLD, nous avons une opportunité et un encouragement pour mettre la barre plus haute en ce qui concerne l'atténuation de l'utilisation malveillante du DNS. Les contrats des gTLD contiennent déjà des dispositions par rapport à l'abus du DNS. Nous pourrions donc mettre en place une mesure similaire, voire améliorée, parce que nous pouvons tirer des leçons de nos expériences passées avec le programme gTLD. Nous pouvons donc améliorer ces mesures. Il y a certes quelques lacunes comme on en a parlé dans d'autres réunions, mais cela pourrait être amélioré pour la deuxième série de nouveaux gTLD, ce qui représente une très bonne opportunité. Voilà donc une prochaine étape possible du point de vue du groupe de travail PDP sur les séries ultérieures de gTLD. On sait que l'utilisation malveillante du DNS doit être traitée dans une vision d'ensemble avec les éléments dont nous disposons.

Un autre point qui a été soulevé et qui fait l'objet de débats porte sur la définition d'abus ou d'utilisation malveillante du DNS. Nous savons qu'il y a beaucoup de points de vue différents, mais il y a également des points d'accord. En septembre 2019, il y a eu une déclaration du GAC concernant l'abus du DNS qui fait référence au langage qui a été utilisé dans d'autres avis du GAC et par certains groupes de parties prenantes. Il est important que les collègues dans la communauté des parties prenantes sachent qu'il y a d'autres propositions de définition d'abus et qu'il y a un grand effort en place par rapport à cette question. Diapositive suivante s'il vous plaît.

Ici, j'aimerais faire référence – je sais que nous n'avons pas encore beaucoup de temps – aux différentes définition d'abus du DNS qui ont

été établies et auxquelles on a fait référence dans l'avis du GAC. L'équipe de révision CCT avait une définition qui parlait des activités non sollicitées, trompeuses et intentionnelles qui utilisent le DNS pour des procédures liées aux noms de domaine ; ensuite, il y a l'abus du DNS qui fait référence à des formes plus techniques ou malveillantes d'activités tels que les logiciels malveillants, le hameçonnage et les réseaux zombies ; ensuite, il y a les contrats de l'ICANN qui font référence à l'abus du DNS de manière plus large, par exemple l'opération de hameçonnage, réseaux zombies, logiciels malveillants, etc. Donc même en utilisant cette définition, nous donnerions beaucoup de marge pour pouvoir atténuer ce type de comportement malveillant.

Je voulais à titre de rappel vous dire qu'il y a déjà des définitions qui ont été établies qui pourraient être utilisées comme base pour le travail qui aura lieu plus tard. Diapositive suivante s'il vous plaît.

Pour ce qui est des prochaines étapes et à un niveau très général, nous encourageons les membres du GAC à participer au travail que réalise la communauté sur la définition de l'utilisation malveillante du DNS. Et on l'a dit à plusieurs reprises dans cette réunion et dans d'autres réunions, le travail qui est fait en particulier par nos collègues de l'ALAC est très utile pour essayer de ne pas nous retrouver avec davantage de victimes des abus du DNS.

Sur ce, je vais demander à Manal si elle est d'accord pour que l'on consacre cinq minutes aux questions et dans le cas contraire si on devrait peut-être reprendre cette partie de la séance à une autre

occasion si on a plus de temps. Mais je voulais en faire autant que possible dans le temps que nous avions. Je vous cède la parole et je vais me contrôler.

PRÉSIDENTE MANAL ISMAIL : Merci beaucoup Laureen. Je comprends tout à fait qu'il y avait beaucoup de contenu à aborder au cours de cette séance. Ceci étant, je suis d'accord pour que l'on réponde aux questions tout de suite. On avait prévu de passer en revue rapidement le communiqué dans la demi-heure qui nous reste, mais nous pouvons essayer de reprogrammer cela demain et nous aurons une autre occasion lors de la séance de demain qui sera consacrée au WHOIS et au EPDP.

Alors pourquoi pas prendre quelques questions de celles qui ont été envoyées. J'en ai vu beaucoup sur le chat. Mais je vois également qu'Olivier lève la main. Alors Olivier, allez-y. Je vais demander à tout le monde que l'on accorde la priorité aux questions du GAC, mais s'il n'y en a pas, on verra s'il y a des questions du reste des participants. Olivier, vous avez la parole.

COMMISSION EUROPÉENNE : Merci Manal, merci de m'avoir donné la parole.

Bonjour à tous. Je voudrais tout d'abord féliciter encore une fois le travail du PWSG. On voit à travers cette séance le niveau du travail qui est fait et il me semble que l'utilisation malveillante du DNS est un sujet très important.

Je tiens en même temps à appuyer les propositions de Shinya du Japon parce qu'il me semble qu'en fin de compte, beaucoup des questions dont nous sommes en train de discuter ici pourraient être résolues à travers la conformité contractuelle avec des obligations contractuelles qui soient appliquées. Je pense que cela a déjà été dit dans un bon nombre de rapports. Il serait très bien d'essayer d'améliorer ces dispositions, mais la conformité et l'application me semble-t-il sont deux outils très importants. Il s'agit d'outils qui permettraient, comme disait Shinya, de pouvoir traiter les cas d'abus, parce que la plupart des parties contractantes suivent les dispositions contractuelles, mais certaines ne font pas suffisamment pour les éviter. Et je pense que c'est ces parties prenantes à qui il faut parler.

Puis, il y a la question de l'exactitude des données d'enregistrement qui est également un outil très important pour pouvoir lutter contre l'utilisation malveillante du DNS. J'étais très intéressé par le rapport de Laurin et j'espère qu'elle le partagera avec tout le monde. Toutefois, elle a confirmé que l'accès aux données d'enregistrement est un outil très important pour les agences d'application de la loi et pour les experts en vie privée ; c'est une question sur laquelle nous avons beaucoup insisté au GAC.

Puis, pour le rapport SSAC115, je sais qu'il contient des recommandations très utiles. Je soutiens fortement le fait que nous puissions le reprendre demain lors de notre réunion bilatérale avec le Conseil d'Administration et voir ce qu'ils en pensent pour voir comment collaborer.

Voilà mes commentaires. Ce n'était pas tellement des questions. Merci Manal.

PRÉSIDENTE MANAL ISMAIL : Merci Olivier. Je vois beaucoup de personnes qui se font l'écho de ce que vous dites sur le chat. Merci au PSWG pour leur travail inlassable pour tenir le GAC au courant de ce qui se passe. J'ai vu un commentaire de l'Inde sur le chat qui dit : « Éduquer les utilisateurs finaux sur l'utilisation malveillante du DNS et sur l'exactitude des données aidera à atténuer l'utilisation malveillante du DNS. Le manque de sensibilisation des utilisateurs finaux vis-à-vis de l'utilisation malveillante du DNS doit être abordé à travers le développement de contenu en différentes langues. Pour ce faire, il devrait y avoir un groupe qui soit formé pour mettre au point ces contenus et pour aider les pays intéressés à se former et à accéder au contenu du cours dans les langues régionales. »

J'ai vu également un lien partagé sur le chat pour pouvoir accéder à du matériel. Je sais que ce sera également évoqué lors de notre réunion bilatérale avec l'ALAC.

Je vais m'arrêter là pour voir s'il y a des commentaires des présentateurs.

LAUREEN KAPIN : Du côté de l'ALAC et du groupe de travail sur la sécurité publique, il y a beaucoup d'intérêt à travailler ensemble sur ces sujets. Et je suis tout à fait consciente du fait que les collègues des unités constitutives des

parties contractantes considèrent également ces questions et on déjà rédigé leurs propres documents. Avec leur énergie et avec l'expertise que nous partageons tous, nous pourrons sans doute pouvoir mettre au point quelque chose, parce que l'idée n'est pas tout simplement de rédiger des documents, mais de faire en sorte qu'ils soient après disponibles en autant de langues que nécessaire pour que toute la communauté puisse en bénéficier. Je pense que ces occasions de collaboration sont très importantes et très prometteuses.

PRÉSIDENTE MANAL ISMAIL : Merci Laureen, oui, très intéressant ce que vous dites, très juste.

Je ne vois plus d'autres mains levées. À ce que je vois, il n'y a plus de questions des collègues du GAC sur le chat. Si je ne les ai pas vues, je vous prie de me les envoyer à nouveau sur le chat ou de lever la main.

En attendant, j'ai vu une question de Dean Marks disant : « Étant donné que l'organisation ICANN semble avoir adopté la position de ne pas être un contrôleur individuel ou conjoint des données d'enregistrement et qu'elle ne peut donc pas mettre en œuvre les exigences d'exactitude des données ou en vérifier l'exactitude, comment est-ce que le GAC prévoit que le service de conformité de l'ICANN aborde les propositions concrètes que le Japon a proposées ? »

LAUREEN KAPIN : C'est une question difficile à répondre. Peut-être que certaines des opinions vis-à-vis de la capacité de contrôle de l'ICANN nous ont

surpris et peut-être faudrait-il que l'on considère la question un peu plus en profondeur. Il faudra voir, mais je pense que ce que dit Dean surtout est que les questions d'exactitude sont importantes et que la question de savoir qui va assumer le contrôle est importante.

Je signalerais à ce point-là les positions de contrats existants qui contiennent des obligations par rapport à l'exactitude. Les contrats existants exigent également l'application robuste des dispositions existantes qui sera sans doute bénéfique. Mais il reste toujours du travail à faire, comme nous le savons tous, étant donné que nous avons déjà des dispositions contractuelles mais que le problème d'exactitude des noms de domaine reste. Et voilà pourquoi d'ailleurs il y a du travail futur qui est signalé par le PSWG, groupe que le GAC suit de près et travail auquel le GAC prévoit de s'impliquer.

PRÉSIDENTE MANAL ISMAIL : Chris.

CHRIS LEWIS-EVANS : Merci Manal. Je voulais ajouter moi-même que malheureusement, les chapitres et les articles du RRA qui abordent la question de l'exactitude diffèrent des dispositions du RGPD. Et comme Laureen l'a dit, il faudrait travailler dessus avec la communauté pour pouvoir ajuster un peu la question. Je sais que le GAC s'est proposé pour aider à compléter cet exercice que la GNSO veut suivre.

PRÉSIDENTE MANAL ISMAIL : Merci Chris. C'était effectivement une question difficile et il est intéressant d'y réfléchir. Mais je sais que la réponse ne vient pas forcément tout de suite.

Puisque nous sommes en train de discuter de la proposition du Japon, je vais moi-même poser une question ici avant de passer au reste des questions. S'il y a une certaine expérience, comment faire la preuve que les noms de domaine ne font pas l'objet d'un cas d'abus ? Parce que je pense que c'était ce sur quoi portait la présentation, n'est-ce pas ? Alors si vous avez des expériences ou des meilleures pratiques à partager dans ce sens, ce serait très utile.

Entre temps, je vais voir s'il y a d'autres questions. J'ai vu une question de Greg qui demandait à Laureen de citer la définition proposée par le GAC de ce qu'est l'utilisation malveillante du DNS. Laureen, vous avez déjà parlé de cela, je pense.

CHRIS LEWIS-EVANS : Manal, Laureen a parlé de la déclaration du GAC concernant l'utilisation malveillante du DNS dont j'ai partagé le lien sur le chat pour pouvoir y accéder.

PRÉSIDENTE MANAL ISMAIL : Parfait, merci. C'est déjà fait.

J'ai vu un autre commentaire de Susan Payne disant : « Laureen, en quoi l'imposition de nouvelles obligations aux TLD qui n'existent pas encore aurait un impact sur ce qui existe déjà ? Les TLD qui ont déjà un

contrat n'auront point d'incitation pour adopter différentes dispositions. Pour rappel, la grande majorité du volume de cas d'utilisation malveillante se fait dans les TLD historiques. Alors pourquoi ne pas se concentrer là-dessus ? »

LAUREEN KAPIN : De très bonnes remarques. Je pense que cette observation d'où se trouvent la plupart des cas d'abus, c'est vrai que c'est dans les TLD historiques. Je parle ici de taille et non pas de portion. La réponse à cette question, sachant que ces observations sont toutes très justes, est que nous faisons de notre mieux lorsque nous le pouvons. Les contrats des TLD hérités ne sont pas à présent en train d'être négociés ; ce qui constitue véritablement un pot d'or est celui des nouveaux gTLD parce que c'est là qu'il nous reste à développer des normes et des contrats et c'est là notre occasion d'améliorer les dispositions.

Y aura-t-il un effet de ruissellement pour la première série de nouveaux gTLD pour les contrats du .com ? Le contrat actuel du .com a adopté certaines des sauvegardes des nouveaux gTLD dans sa révision du contrat. Alors oui, je dirais que cela a ce potentiel d'impacts positifs à travers les retombées, mais il faut saisir les occasions qui se présentent. Vous savez que le parfait est l'ennemi du bien.

Moi, j'adorerais pouvoir m'occuper des problèmes d'utilisation malveillante sur tous les TLD tout de suite, dès que possible, mais il faut être conscient du fait que tout n'est pas toujours possible et que

parfois, le travail progressif permet d'avancer plus constamment. Il serait très bien de pouvoir avoir un effet boule de neige, mais en attendant que cela se passe, je vais me conformer avec les possibilités qui se présentent et c'est de travailler sur la prochaine série de nouveaux gTLD.

PRÉSIDENTE MANAL ISMAIL : Merci Laureen.

Désolée si je n'ai pas vu à toutes les questions. Je ne pense pas qu'il y en ait d'autres.

Merci d'avoir partagé le lien à l'enquête sur le chat, Laurin. Je pense qu'elle est très intéressante et très informative. Je me demandais s'il y avait également des questions concernant les solutions potentielles, surtout pour ceux qui étaient insatisfaits. Est-ce qu'il y aura des possibilités de partager d'autres solutions ? Cela pourrait être intéressant.

LAURIN WEISSINGER : Merci beaucoup.

C'est un sujet que nous allons aborder sans doute, parce que nous allons nous y pencher avec le CPWG pour essayer d'explorer de possibles solutions et nous allons revenir vers vous avec un document où il y aura ces suggestions. D'abord, nous collectons des données pour pouvoir nous y pencher. Comme vous avez pu le voir, Gabe a fait quelques observations par rapport aux données et par rapport à ce

qu’elles nous communiquent. Faire un rapport des données collectées n’est pas tout à fait la même chose qu’apporter des suggestions. Donc nous allons nous pencher sur ces données pour élaborer des suggestions ou des recommandations.

PRÉSIDENTE MANAL ISMAIL : Merci beaucoup à tous nos intervenants du CPWG ainsi qu’aux intervenants du PSWG pour cette séance qui a été très informative. Ceci conclut notre séance et notre discussion sur l’utilisation malveillante du DNS.

Pour les collègues du GAC, je vous prie de rester dans la salle, nous allons profiter des quelques minutes qu’il nous reste pour avoir un aperçu du communiqué. Merci à tous. Le personnel de soutien, s'il vous plaît, dites-moi quand nous pouvons commencer nos discussions sur le communiqué. Merci beaucoup.

[FIN DE LA TRANSCRIPTION]