ICANN76 | Forum de la communauté – ccNSO: point du Comité permanent sur l'utilisation malveillante du DNS
Mercredi 15 mars 2023 – 15h00 à 16h00 CUN

BRENDA BREWER: Nous allons lancer l'enregistrement et lancer la séance. Bonjour et bienvenue à cette séance sur l'utilisation malveillante du DNS. Je m'appelle Brenda et avec Devan et Andréa nous sommes les responsables de la participation à distance pour cette séance.

Veuillez noter que la séance est enregistrée et est régie par les normes de comportement attendues pas l'ICANN. Au cours de cette séance les questions et commentaires ne seront lus à haute voix que s'ils sont formulés correctement, comme indiqué dans le chat. Je lirai les commentaires et questions pendant la durée fixée par le président ou le modérateur de cette séance.

L'interprétation pour cette session comprendra l'anglais, l'espagnol, le français et l'arabe.

Cliquez sur l'icône d'interprétation dans Zoom et sélectionnez la langue que vous écouterez dans la séance. Si vous souhaitez prendre la parole, levez la main dans la salle Zoom et une fois que l'animateur de la séance aura dit votre nom ouvrez votre micro et prenez la parole.

Avant de prendre la parole, assurez d'avoir sélectionné la langue dans laquelle vous vous exprimerez dans le menu d'interprétation. Veuillez indiquer votre nom pour l'enregistrement et la langue dans laquelle

vous vous exprimerez si vous parlez une autre langue que l'anglais. Quand vous parlez pensez à mettre en sourdine tous les autres appareils et notifications. Veuillez parler clairement et à un rythme raisonnable pour permettre une interprétation précise.

Cette séance comprend une transcription automatisée en temps réel, veuillez noter que cette transcription n'est pas officielle et ne fait pas autorité. Pour la visualiser, veuillez cliquer sur le bouton « close cpation » dans la barre d'outils Zoom.

Pour assurer la transparence de la participation au modèle multipartite de l'ICANN, nous vous demandons de vous connecter aux sessions Zoom en utilisant votre nom complet, par exemple un nom et un prénom. Vous risquez d'être exclu de la séance si vous n'utilisez pas votre nom complet.

Sur ce, je donne la parole à Nick Wenban-Smith.

NICK WENBAN-SMITH: Merci beaucoup et bienvenue à cette séance du comité permanent de la ccNSO sur l'utilisation malveillante du DNS. Je suis Nick de .UK. Il s'agit d'une sous-commission formée par le conseil de la ccNSO en avril 2022. Et nous sommes très heureux d'avoir bien avancé et d'avoir déjà des résultats à vous présenter. J'espère que nous aurons un dialogue tout à fait constructif et engageant.

Je pense qu'il est important que la ccNSO ait son propre leadership, sa propre voix dans ce domaine de l'utilisation malveillante du DNS.

Et, pour revenir un petit peu en arrière par rapport aux termes de références, il est important d'être très clair sur ce qui n'est pas dans notre portée, notre cadre de référence. Nous sommes là pour avoir un forum pour parler de l'utilisation malveillante du DNS. C'est une préoccupation de la communauté tout entière. Et, très clairement, notre mission en tant que comité permanent pour les ccTLD, on n'en a pas encore beaucoup parlé, mais c'était une question de perception également. Donc on en parlait peu publiquement, mais on y travaillait.

Et je crois que l'objectif c'est de remédier, justement, à ce problème. Ceci dit, nous ne sommes pas ici comme le conseil de la GNSO pour formuler des politiques, ce n'est pas notre mandat, c'est de faire prendre conscience dans notre communauté, au niveau des messages, au niveau des indicateurs, d'avoir un meilleur objectif, des indicateurs pour pouvoir parler de ces problématiques.

J'aimerais dire également que dans le cadre des termes de référence, nous voulons avoir ce dialogue tout à fait constructif. Moi je n'aime pas beaucoup le silence. Donc j'encouragerai tout le monde à prendre la parole rapidement durant la réunion, ce sera plus efficace, plutôt que d'attendre.

Donc engageons-nous rapidement dans une conversation. Merci également de vous mettre sur Zoom, comme cela nous pourrons suivre de plus près vos questions/réponses et interventions et je ferai de mon mieux pour gérer les horaires et gérer également tout ce qu'il se passe sur la salle Zoom.

Donc c'est un sous-groupe tout à fait important, le sous-groupe du référentiel DAC sur l'utilisation malveillante du DNS. Et ensuite nous aurons la possibilité d'avoir des questions et réponses.

Je vais donner la parole à David qui va nous parler de ce référentiel.

DAVID MCAULEY: Je suis un employé de VeriSign et je participe à la ccNSO et à ce comité puisque nous gérons .CC. Et je suis ici en tant que personne principale du sous-groupe référentiel, donc en ce qui concerne ce comité permanent sur l'utilisation abusive du DNS.

Nous allons parler de deux projets d'informations pour les gestionnaires de ccTLD et je vais bientôt donner la parole à mes collègues.

FERNANDO ESPANA: Je vais m'exprimer en espagnol. Bonjour à tous, je suis Fernando Espana, j'appartiens à GoDaddy et aujourd'hui nous allons travailler sur le sous-groupe du référentiel du DASC. Dans ce sous-groupe nous avons deux projets sur lesquels nous travaillons.

Le premier est la création d'un référentiel de liens utiles sur l'utilisation malveillante du DNS et autres ressources pour les gestionnaires de ccTLD. Ce projet est celui qui est actuellement en cours de réalisation.

Le deuxième projet vise à créer une liste de courriels électroniques consacrés à la ccNSO pour qu'ils soient ensuite utilisés par les gestionnaires de ccTLD pour échanger des informations liées à l'utilisation malveillante du DNS.

Ce projet va continuer, une fois que le premier projet sera terminé.

Je redonne la parole à mon collègue David qui va vous donner davantage d'informations sur le reste de notre présentation. Merci.

DAVID MCAULEY: Merci beaucoup, Fernando. Merci. Nous allons passer à la diapo suivante.

Vous pouvez voir les informations à la l'écran. À la base, ce que nous faisons dans ce groupe est de créer un référentiel d'informations qui seraient utiles pour les gestionnaires des ccTLD pour les membres de la ccNSO également. Et nous allons commencer par obtenir ces informations et les diffuser auprès des gestionnaires de ccTLD. C'est un groupe qui sera peut-être plus large à l'avenir, mais nous voulons le lancer avec solidité. Et tout cela sera fait sous les hospices groupes qui sera établi, ce sera un conseil éditorial si vous voulez. Je vais en parler un peu plus, cela est sujet à l'approbation du conseil.

La diapo suivante nous indique que le DASC contrôlera cela, nous lui ferons rapport et nous aurons ce conseil éditorial qui sera là pour s'assurer que nous avons les bonnes informations dans notre référentiel. Vous pouvez voir en bas qu'il y a 4 points et il s'agit là des informations des catégories que nous recherchons pour diffusion auprès de nos collègues. Ce seront des présentations et rapports. Par exemple, il y avait un rapport sur l'utilisation malveillante du DNS, une nouvelle étude sur l'utilisation malveillante du DNS, beaucoup de choses sont publiées. On donnera donc des liens hypertextes pour y avoir accès, décrire un peu ces présentations et rapports.

Ensuite nous voulons également avoir une catégorie d'outils. Des outils utiles pour les responsables des ccTLD pour gérer ces utilisations malveillantes du DNS et ses problématiques. Nos collègues de l'Institut qui étudient l'utilisation malveillante du DNS, à [inaudible] il y a des outils de rapports pour les utilisations malveillantes. Et il y a également le compas DNS Abuse, sur l'utilisation malveillante du DNS, les logiciels malveillants, etc. nous aurons accès à ces outils par ce biais.

Troisième point : définition et politiques. Comme vous le savez, nous avons vu cette conversation à l'ICANN se développer, il n'y a pas une seule définition ou approche pour comprendre l'utilisation malveillante du DNS. Et donc nous vous donnerons accès à ces définitions que nous pensons pertinentes.

Quatrièmement, nous aurons également des points sur des articles et des commentaires qui sont également très nombreux, des publications comme [inaudible], des commentaires tout à fait intéressants sur l'utilisation malveillante du DNS et parfois même dans les journaux et la presse, nous trouvons des informations et des articles.

Donc nous allons considérer tout cela et faire de notre mieux pour référencer tout ce qui est pertinent pour nos collègues de la ccNSO. Et ce sera un travail fait sous l'égide du comité permanent.

Donc nous aurons toutes ces informations qui seront fiables, nous allons promouvoir ce contenu fiable, ces sites web, nous allons indiquer à quel point cela peut être utile, nous allons accroitre l'accès à cela et nous allons archiver tous ces points en temps et en heure, selon l'urgence, selon les dates de publication, et nous resterons en contact

avec le DASC et avec la communauté ccNSO qui sera informée constamment de l'évolution de notre référentiel.

Voici donc les membres de ce sous-groupe référentiel, vous pouvez nous contacter, n'hésitez pas, nous contacter en tant que groupe ou individuellement. N'hésitez pas à réagir sur ce qui a été dit.

J'aimerais remercier tous les membres de l'équipe dont vous voyez les noms à l'écran. Comme l'a dit Fernando, une fois que tout cela sera fini nous aurons une liste de diffusion pour diffuser tout cela et je suis prêt maintenant à répondre à vos questions.

NICK WENBAN-SMITH: Merci beaucoup, David. Maintenant nous passons aux questions. Est-ce que vous avez des questions à poser à ce sous-groupe ?

Je crois qu'on peut les faire à travers Zoom aussi. Pour le moment il n'y a pas de question dans Zoom.

Ha, il y a une question ici de John McCormick : est-ce que vous avez considéré la possibilité d'ajouter des détails concernant des TLD qui ont des offres de réduction lorsqu'il y a des enregistrements avec des corrélations, lorsqu'il y a une corrélation entre ces enregistrements.

C'est quelque chose qui vient du sous-groupe, je crois que c'est une question intéressante qui correspond vraiment à la question liée à ce sous-groupe. Peut-être que… David, qu'en pensez-vous ? C'est une question pour le sous-groupe.

DAVID MCAULEY: Ce n'est pas vraiment encore une question que nous avons abordée, nous pouvons la considérer. On va la présenter à notre groupe, on pourra y répondre.

Ce que je veux dire ici c'est que notre objectif, avant tout, est de commencer, mettre les choses en place. Ensuite nous verrons dans le futur un travail un petit peu plus sophistiqué et avancer un peu dans ces questions.

Merci, John, je prends note de votre question qui va apparaitre dans l'ordre du jour de notre prochaine réunion, et nous y répondrons.

Est-ce qu'il y a d'autres questions dans Zoom ou dans la salle ?

NICK WENBAN-SMITH: Et bien je ne vois pas d'autres questions, nous allons passer au point suivant de l'ordre du jour, à savoir le travail du deuxième sous-groupe qui travaille sur l'enquête qui a été réalisée. C'est un plaisir vraiment de présenter ce thème pour moi.

Nous avons un groupe de collègues qui a fait un très bon travail dans ce sous-groupe lié à l'enquête, avec beaucoup de données très riches, beaucoup de participation de la part de la communauté, nous sommes très satisfaits d'ailleurs.

Et si vous voyez ici, est-ce que l'on peut passer à la prochaine diapositive s'il vous plait ?

Donc voilà, cette enquête, l'ensemble des données, 57 ccTLD ont donné des réponses uniques ce qui représente 100 ccTLD sur un total de 316

qui ont été délégués. Il n'est pas obligatoire de participer à ces enquêtes, bien sûr, mais de voir ce taux de réponse nous a permis de comprendre que certains ccTLD ne pouvaient pas participer à ce type d'enquêtes pour différentes raisons parce qu'ils avaient leur processus interne, leur structure et leur mécanisme de gouvernance. Donc on ne peut pas parvenir à 100 % de réponses dans ces cas-là. Mais nous avons donné aux personnes qui ont répondu à l'enquête la possibilité de rester anonymes ou de faire une déclaration publique. Et nous avons respecté cela. Je pense que cela a aidé aussi à obtenir davantage de participations de la part de ceux qui ont répondu à cette enquête.

Prochaine diapositive.

Alors en ce qui concerne les données démographiques je vais donner la parole à un de mes participants à distance, un membre du sous-groupe qui participe énormément, il s'agit d'Angela du ccTLD du Botswana.

ANGELA: Merci, Nick. Est-ce que vous m'entendez bien ?

NICK WENBAN-SMITH: Oui, on vous entend très bien. Allez-y.

ANGELA: Parfait. Bonjour, bonsoir à tous. Je salue tout le monde, buenas tardes puisque vous êtes à Cancún.

Nous allons voir un peu les données démographiques. Je vais vous présenter ce qui fait que le ccTLD ici est différent. Nous répétons cette

notion selon laquelle les ccTLD sont quelque chose qui ne correspond pas vraiment dans tous les cas, on ne peut pas avoir une seule option.

Ce que je voudrais ici vous dire, un point qui me parait important concernant l'enquête, c'est que nous analysons l'utilisation malveillante du DNS comme étant un sujet qui ne respecte pas les frontières. Par conséquent, l'utilisation malveillante du DNS, le cybercrime en général est quelque chose qui peut toucher tout le monde, affecter tout le monde partout dans le monde, à partir du moment où on est connecté à internet.

Ce que cette enquête montre bien c'est que, quel que soit le pays, le ccTLD, le ccTLD peut jouer un rôle important concernant l'utilisation malveillante du DNS et la lutte contre cette utilisation malveillante. En fonction des régions : les réponses venaient de l'Europe, suivi par l'Amérique du Nord.

Nous avons fait aussi une enquête sur les modèles de gouvernance des ccTLD. Nous avons utilisé l'étude qui avait été présentée par l'ancien président de la ccNSO, Kathrina, et on s'est rendu compte qu'il y avait aussi d'autres points importants, c'est-à-dire les compagnies qui étaient limitées par les garanties et les membres qui travaillaient dans les organisations statutaires. Nous avons eu un modèle de registre aussi sur lequel nous avons travaillé et vous voyez ici que le plus grand nombre de réponses viennent du modèle bureau d'enregistrement, titulaire de registre, mais aussi des trois enregistrements directs, ou du système d'enregistrement direct.

Prochaine diapositive.

Nous avons aussi fait un classement concernant les différents aspects du ccTLD et les domaines enregistrés. Donc à partir des réponses reçues, nous constatons que plus d'un million de domaines ont été enregistrés mais qu'en moyenne on avait environ 10 000 domaines. On a aussi regardé les tailles en termes du nombre d'employés que chaque ccTLD avait et nous avons constaté qu'il y avait beaucoup de diversité dans ce domaine et qu'il y avait en général une cinquantaine d'employés ou plus. Comme vous voyez ici le graphique, il y a différentes combinaisons ici. On constate que malgré les tailles il y a des ccTLD qui sont encore capables d'enregistrer ou de surveiller l'utilisation malveillante du DNS. Et on voit que deux personnes qui ont participé à l'enquête ont indiqué qu'ils avaient un employé au sein de leur ccTLD.

Nous avons aussi regardé les utilisations malveillantes qu'ils avaient constatées et les atténuations pour voir s'ils avaient des compétences dans ces ccTLD pour lutter contre l'utilisation malveillante du DNS, ou si ces ccTLD utilisaient seulement des employés normaux au niveau administratif.

On a constaté que 75 % des personnes qui répondaient indiquaient qu'ils n'avaient pas de personnes spécialisées dans le domaine de l'utilisation malveillante du DNS qui travaillent dans leur ccTLD.

Ici nous avons analysé les législations concernant la protection de données et la possibilité qu'elles affectent les ccTLD quand on parle d'utilisation malveillante du DNS. On a constaté que plus de 60 % des personnes qui ont répondu ont dit qu'ils étaient affectés par ces législations.

Et, dans la partie du texte libre, on leur demandait de nous dire dans quelles mesures ces législations qui les affectaient.

Les ccTLD ont aussi indiqué qu'ils participaient à un certain type de collaboration, plus de 80 % des participants à l'enquête collaborent avec des équipes de réponses en cas d'incident de sécurité, d'agence de force de l'ordre et autres. Des fois on a une combinaison de toutes ces organisations, de tous ces organismes.

On a aussi regardé le pourcentage de l'utilisation malveillante du DNS auquel les ccTLD ont été exposés. La plupart des réponses indiquaient un pourcentage inférieur à 0,05 %. Et lorsque l'on regarde ces chiffres, on se rend compte que cela dépend de la taille elle-même du ccTLD. Il y a certains ccTLD qui ont un pourcentage de 0,05 % mais cela représente des millions des fois. Donc même si ces pourcentages sont bas, il faut se rendre compte que cela peut venir de ccTLD qui ont énormément de domaines ou moins de domaines et à ce moment-là on va avoir un chiffre qui va être modifié.

Au niveau des résultats de l'enquête on a constaté que beaucoup de participants ont indiqué qu'ils n'étaient pas sûrs du type d'utilisation malveillante qu'ils avaient eue et s'ils les avaient tous enregistrés.

J'en ai terminé avec ces chiffres, je vous rends la parole.

NICK WENBAN-SMITH: Merci beaucoup, Angela. Nous allons passer à la prochaine diapositive et nous allons donner la parole à Bruce qui va nous parler des différents aspects d'utilisation malveillante du DNS.

BRUCE TONKIN: Je vais parler en anglais et j'espère que tout le monde me comprendra vu mon accent.

En termes de types d'utilisation malveillante du DNS, vous voyez ici les différents aspects. Nous avons eu 57 réponses ici dans ce domaine, 29 qui indiquaient qu'il s'agissait pour la plupart des participants. On voit qu'au niveau des personnes qui ont répondu on a ceux qui appartiennent à la communauté des gTLD, avec des problèmes de logiciels malveillants, hameçonnage, réseaux zombie et dévoiment. Ensuite on a des actions qui sont moins prises dans le domaine des pourriels. Donc on voit que pour la communauté des ccTLD on est un petit moins proactif pour les pourriels.

Au niveau des contenus, on constate que plus de la moitié de ceux qui ont répondu ont pris des actions mises en œuvre, des actions quand il s'agissait de matériel lié à l'abus sexuel contre des enfants. En général, on a constaté que ces ccTLD avaient agi dans ces domaines.

En ce qui concerne cette utilisation malveillante, nous avons la question de terrorisme éventuel, de cyberharcèlement, les pourcentages sont beaucoup plus bas. C'est moins de 25 % de taux de réponse. Et lorsque l'on fait une corrélation avec les données des ccTLD, on voit que les organisations sont intégrées verticalement à ce niveau et gèrent dans le cadre juridique cette utilisation malveillante du DNS. Dans d'autres pays, c'est beaucoup plus séparé.

Il y a des opérateurs de registre qui ont un mandat limité mais il y a d'autres organisations dans le pays qui sont responsables de cela, de

cette lutte contre l'utilisation malveillante. Donc c'est une réponse qui s'ensuit de la part des ccTLD.

Donc, très souvent, cela est en lien avec les mécanismes de notification, notamment.

Sur la droite, vous avez infractions aux marques, les marques déposées. Vous pouvez voir ces chiffres. La plupart des opérateurs prennent des mesures, mais en fait la plupart des opérateurs font des réponses écrites à cela et il y a des systèmes de services indépendants de résolution des litiges. Il y a différents modèles qui existent pour les gTLD et les opérateurs de registre de cc ont ce type de réponses et prennent des décisions indépendantes et gèrent les litiges de ce type.

Diapo suivante.

Alors, voyons le type d'atténuation pour cette utilisation malveillante du DNS. Ces chiffres nous indiquent que nous avons en effet des procédures pour le dépôt des plaintes. Il y a beaucoup de ccTLD qui utilisent la sensibilisation de la clientèle pour que l'on comprenne bien les différents types d'abus qui existent. Les différents outils, par exemple, il y a une certaine forme de renseignement et d'intelligence au niveau de l'utilisation malveillante.

Il y a également des procédures, une fois qu'il y a un enregistrement de noms de domaine, il y a des commentaires écrits, il y a des vérifications qui sont fournies après l'enregistrement et il y a des tendances qui sont observées et suivies. Et une majorité des codes pays ont des politiques d'inscription qui luttent contre le hameçonnage par exemple, il y a des rapports rapidement sur les sites de hameçonnage et il y a des décisions

qui sont prises. Il y a le rapport avec les mécanismes de notification de confiance, qui sont très souvent locaux. Au niveau national il y a des équipes d'intervention lorsqu'il y a des problèmes de sécurité informatique. Il y a également les forces de l'ordre qui peuvent jouer un rôle à ce niveau. Et je crois qu'il faut mieux comprendre les systèmes de mécanisme de notification de confiance lorsque cela est placé en dehors du pays. Et il y a une question d'acceptation de la communauté à ce niveau.

Et, enfin, sur la droite, vous avez l'éducation, l'information des bureaux d'enregistrement et des titulaires de nom de domaine en rapport avec l'utilisation malveillante du DNS. On n'en parle pas beaucoup et je crois que peut-être uniquement la moitié font de la sensibilisation à ce niveau. Donc nous pouvons en parler plus pour renforcer ces points d'information et de sensibilisation.

Diapo suivante.

Très bien. Cela c'est tout à fait intéressant. Les chiffres que j'ai mentionnés auparavant montraient que les personnes ayant répondu avaient des mécanismes locaux de notification de confiance, mais il n'y avait pas beaucoup d'accords qui existaient et d'accords formels. Donc c'est en général très informel que l'on choisit de prendre en compte les informations provenant des mécanismes de notification de confiance.

Donc s'il y a détection d'utilisations malveillantes, des actions sont prises, mais 31 personnes ont répondu que l'approche dépend du résultat de notre évaluation des risques. Très peu prennent des mesures uniquement à la suite d'une notification. Donc ils vérifient qu'il y a bien

eu un problème avant de prendre véritablement des mesures. Et cela est indiqué, l'approche dépend des résultats de l'analyse qui est effectuée.

Enfin, sur la droite, vous voyez que la plupart d'entre nous ont des mécanismes en place pour que les membres du public effectuent des rapports sur l'utilisation malveillante du DNS.

TATIANA TROPINA: Donc ce que vous avez vu sur l'écran, c'est beaucoup de chiffres. Mais ce qui est très intéressant, je pense, c'est d'aller au-delà des statistiques, des chiffres. Une suis conseillère à la ccNSO. Il y a beaucoup de mécanismes de rapports qui ne nous montrent pas la diversité des efforts d'atténuation en cas d'utilisation malveillante du DNS de la part des ccTLD.

Il y a une grande variété de mécanismes, il y a des rapports qui sont faits par courriel, des rapports types de sites web. Et, d'une manière intéressante, on peut voir également le rôle des agences, notamment de l'équipe d'intervention notamment en cas d'incidents liés à la sécurité informatique. Il y a des mécanismes de rapport liés à ces institutions et il y a une indication de ces abus du DNS. Et on essaye de faire en sorte que le grand public fasse appel, notamment, aux forces de l'ordre. Il y a donc plusieurs manières de réagir.

Je vais revenir sur ce qu'a dit Bruce. J'essaye de voir… Je ne vois plus la diapo. Je ne sais pas où on en est.

Ce dont j'allais parler, jusqu'à ce qu'apparaisse la prochaine diapo à l'écran, ce sont les actions prises par la ccTLD, les différents mécanismes

qui existent lorsqu'il y a des demandes des forces de l'ordre pour retirer, par exemple, un nom de domaine. Vous l'avez vu vous-même, il y a plusieurs manières de procéder, vous pouvez faire votre diligence raisonnée, vous pouvez prendre en compte ces demandes. Mais en général il y a des efforts de diligence raisonnée au niveau du ccTLD pour s'assurer qu'il y ait bien une utilisation malveillante du DNS.

Je ne vois pas la diapo, est-ce que je dois continuer ? Je vais dire prochaine diapositive.

Quelques commentaires. Lorsqu'on parle de diligence raisonnée et lorsqu'on nous dit que…

Nous allons devoir changer de diapo, voilà.

Une nouvelle fois, lorsqu'on voit cela d'une manière plus granulaire, plus en détail, lorsque les ccTLD n'ont pas de diligence raisonnée il y a néanmoins des vérifications et contrôles qui sont effectués et il y a des requêtes qui leur arrivent, à ces ccTLD, et ils vérifient par exemple que ce n'est pas une faute typographique sur le nom de domaine qui a été effectué. Donc la diligence raisonnée ne veut pas dire qu'il n'y a pas de vérification qui soit effectuée.

Je vais passer à la prochaine diapo et passer la parole à Bruce.

BRUCE TONKIN: Oui, il y a beaucoup d'outils qui sont utilisés et nous les avons mis sur ce transparent. Cela va arriver, je pense. Je crois qu'il y a des outils commerciaux, des outils gratuits, des outils en open source. Et il y a une liste de domaines qui ont effectué des rapports. Et, au niveau des

services plus commerciaux, ce sont des organisations à but non lucratif, très souvent. Parfois il faut payer pour avoir accès aux données et pour couvrir leurs frais d'opération.

Au niveau des services plus commerciaux, ce que vous obtenez c'est avoir une liste de domaines, également des informations sur le type d'abus et d'utilisations malveillantes. Est-ce que c'est du hameçonnage, par exemple. Cela nous indique que tel nom de domaine fait beaucoup d'hameçonnage. Mais il y a toujours besoin d'une diligence raisonnée pour faire l'URL, les problèmes de typographie ou autre. C'est ce qu'on obtient au niveau des outils commerciaux.

Il y en a d'autres qui sont simplement des listes de noms qui correspondent à es URL et à des adresses internet. Il y en a qui ne fournissent qu'un service et non pas des données. Donc vous pouvez choisir d'être gérés par ces outils commerciaux en ce qui concerne ces questions d'utilisation malveillantes. Donc plutôt que de faire vous-même des mesures, vous pouvez externaliser cela avec ces outils commerciaux. Vous avez donc le choix.

Il y a également des outils de gestion de cas qui sont disponibles. Pour avoir un cas, ouverture de cas, système de tickets, de numération, d'indexation.

Et, à l'avenir, nous pourrions travailler, en creusant un petit peu plus sur ces thématiques et je pense que la ccNSO sera très intéressée par l'utilisation de ces outils et de voir quels sont ces outils qui sont des plus efficaces.

TATIANA TROPINA: Je voulais parler des instruments commerciaux et open source. Je vais vous en parler même si on ne voit pas la diapo. Le choix entre ces outils, que nous disent les ccTLD ? Cela dépend de leur fonctionnalité. Les ccTLD indiquent que ces outils open source peuvent être très utiles, mais il faut qu'il y ait une centralisation. Les outils commerciaux ont des fonctionnalités beaucoup plus fortes et vous pouvez avoir des services supplémentaires.

Nous avons vu que beaucoup des ccTLD utilisent les deux en fait, les outils commerciaux et les outils gratuits, parce que la diversité est la clef et est tout à fait utile.

Je vais parler de ce qui a été les résultats principaux de cette enquête. Nous allons continuer dans la présentation.

Le dernier, mais non des moindres, explique pourquoi nous devons dépasser les chiffres, pourquoi nous devons dépasser les réponses que nous avons obtenues. Il faut savoir qui va décider d'agir. Et la manière dont les ccTLD et les gestionnaires de ccTLD gèrent l'utilisation malveillante du DNS, ce ne sont pas seulement des procédures internes, les outils utilisés, les réactions que vous avez, c'est en fait dans beaucoup de juridiction dépendant des facteurs externes et beaucoup dépend du contexte juridique.

Parfois les textes de loi établissent d'une manière très stricte ce que vous pouvez faire et ne pas faire. Donc cela dépend de l'envergure de l'utilisation malveillante par exemple, est-ce que c'est criminel ?

Certains des ccTLD ont indiqué que tout ce qui est criminel et qui est lié à l'utilisation d'un nom de domaine va être considéré comme une utilisation malveillante du DNS. Mais des fois le ccTLD ne peut pas prendre d'action ou les mettre en œuvre, à moins qu'il ait vraiment des autorités compétentes ou des forces de l'ordre qui le lui indiquent. Et, à notre avis, cela montre cette idée selon laquelle il n'y a pas une seule solution qui peut s'adapter aux besoins de tous.

Je redonne la parole à Angela.

ANGELA: Prochaine diapositive. Je crois que c'était la dernière.

NICK WENBAN-SMITH: On a besoin d'un petit instant pour régler la partie des diapositives. Nous avons quelques questions dans le chat portant sur l'ICANN et ce qu'il va faire concernant les cas où on a des ccTLD qui ont une activité malhonnête.

Bien, ce n'est pas dans le cadre des termes de référence de notre groupe de travail et c'est un problème pour lequel l'ICANN n'établit pas de politique dans le cadre des codes géographiques. Cela dépend des gouvernements et de leur juridiction.

Cela dit, dans le cadre de notre travail nous avons voulu montrer quels étaient les comportements et pratiques dans ces domaines de manière à pouvoir organiser un débat sur la façon dont nous considérons les choses. À la ccNSO, nous voulons encourager les bonnes pratiques, les bons comportements, nous voulons aider les gens à hausser la barre et

à augmenter le niveau des normes appliquées. C'est pour cela que nous souhaitons avoir cette conversation, ce dialogue et sur la base de données. C'est pour cela que nous faisons ces enquêtes et ce travail.

Donc la ccNSO travaille comme cela et c'est ce que je voulais dire, merci.

ANGELA: Est-ce que nous pouvons continuer ?

NICK WENBAN-SMITH: Oui, allez-y Angela, excusez-nous.

ANGELA: Bien, prochaine diapositive. Je crois qu'après tout ce qui a été dit, d'après ce que Tatiana a dit, on voit qu'il y a des chiffres ici qui indiquent ce qu'il se passe. Mais dans le cadre du ccTLD, il pourrait y avoir davantage de méthodes d'atténuation.

Nous avons pu conclure des réponses que nous avons reçues qu'il y a différents ccTLD dans différentes régions qui participent et appliquent des méthodes ou des politiques telles que des outils de sensibilisation, etc. Mais, malgré cela, tous les ccTLD n'ont pas la possibilité d'accéder à ces ressources lorsqu'il s'agit d'atténuer l'utilisation malveillante du DNS.

Voilà, c'est la conclusion à laquelle nous sommes parvenus. Nous devons continuer à recueillir des informations sur ce thème pour continuer à analyser le secteur.

NICK WENBAN-SMITH: Merci, Angela. Quelques questions ont été envoyées dans le chat. Nous vous remercions. Si nous pouvons passer à la prochaine diapositive s'il vous plait.

Alors, nous avons ces données et, comme je l'ai dit au début, beaucoup de personnes qui ont répondu ne voulaient pas que leurs réponses soient publiées. Notre groupe de travail a continué à analyser cela et veut continuer à approfondir ces questions pendant les 6 ou 12 prochains mois.

Nous allons refaire une enquête et nous allons essayer de voir quelle est l'évolution des différentes politiques et pratiques depuis le début de notre travail.

Une des questions que je vois dans le chat porte sur la relation entre les offres de réduction et les abus de DNS. Alors on peut dire qu'il y a une relation entre certaines promotions faites par les bureaux d'enregistrement et certains gTLD. On a constaté qu'il y avait une corrélation entre des promotions de prix, des réductions de prix et une augmentation des utilisations malveillantes. C'est un des domaines dans lequel nous avons identifié certains de ces points.

Pour l'enquête, nous n'avons pas ces informations, j'ai quelques données, mais je sais que dans la région européenne il y a quelques opérateurs de registre, je vois par exemple mon ami de l'Allemagne, d'autres amis du Royaume-Uni, nous savons qu'en Angleterre et en Allemagne il y a un marché très compétitif avec de très bons prix. Nous

avons de très bons niveaux d'utilisation malveillante du DNS, ils sont très bas.

Donc je crois que c'est intéressant de se demander pourquoi on a cette situation, pourquoi certains ccTLD, gTLD, qui appliquent les lois en général ont des niveaux très bas d'utilisations malveillantes du DNS. Donc on peut se demander ce qui fait qu'on a ces résultats, pourquoi. Je pense qu'il ne faut pas avoir peur de se lancer dans certaines conversations difficiles.

Donc je suis d'accord, le prix peut être en relation avec le taux d'utilisation malveillante du DNS, de toute façon ce n'est pas systématique, mais c'est intéressant comme thème.

Je dirais que ceux d'entre nous qui sont ici et qui savent, qui connaissent leurs responsabilités en tant que serveur pour l'intérêt public savent également qu'ils doivent lutter contre différentes utilisations malveillantes du DNS et qu'il y a une question de réputation aussi pour eux, dans leur activité, au niveau de leur communauté nationale. Et je pense que c'est un point très important.

Notre activité se base sur une bonne réputation, c'est très important. Et nous voulons améliorer le niveau de résultats dans ces domaines et donc c'est important que cette conversation soit prise en compte et qu'on parle de cette question avec tous les ccTLD, c'est un dialogue important qui doit avoir lieu au sein de notre communauté.

En termes d'autres types de travail, je crois que l'on comprend tous la relation entre les opérateurs de registre et les bureaux d'enregistrement, il y a un travail très important ici qui existe au niveau

de l'équipe qui existe entre ces deux organismes. Il faut collaborer et travailler en commun de manière coordonnée avec les bureaux d'enregistrement. Et je crois qu'on sait tous que certains types d'utilisation malveillante et parfois même la grande majorité proviennent plutôt du fait que les bureaux d'enregistrement participent à des actions qui ont beaucoup plus d'impacts que les actions que les opérateurs de registre pourraient mettre en œuvre.

Donc, ici, on a un point important avec des contenus, par exemple dans le cas du contenu abusif pour lequel l'opérateur de registre ne peut pas faire grand-chose.

Un autre thème est aussi la question des outils, parce qu'il y a beaucoup d'outils qui sont payants, d'autres outils qui sont en open source et qui sont gratuits.

Donc je crois que connaitre ces outils et connaitre la sélection d'outils qui existent, les critères d'utilisation de ces outils, quels sont les outils pour lesquels il vaut mieux investir, je pense que tout cela est très important aussi et qu'il y a aussi beaucoup d'outils pour lesquels on dépense beaucoup alors qu'ils ne sont pas vraiment faits spécifiquement pour des opérateurs de registre. Il y a certaines limitations dans ce domaine. Il y a aussi les listes de blocage de réputation qui sont utiles.

Mais, de nouveau, il y a beaucoup de faux positifs. Donc on essaye de mettre en œuvre des actions. Mais je dirais que cela demande beaucoup de temps. Voilà.

Pablo a la main levée, mais je crois qu'il a de nouveau baissé la main, donc… Pablo, vous aviez une question ?

PABLO: Oui. D'abord je voulais féliciter le comité permanent sur l'utilisation malveillante du DNS, pour le travail que vous avez fait et pour cette fantastique présentation que vous venez de nous faire. Donc bravo à vous tous. Et puis je voudrais partager un commentaire concernant une stratégie qui a été utilisée par l'organisation locale et régionale LACTLD à travers laquelle, avant la pandémie, et je parle de quelques jours avant la pandémie, on était ici à Cancún et on a eu la possibilité de travailler avec des juges, des avocats, des représentants de la police de différents pays, on a pu leur présenter ce que l'on voyait. On a eu la possibilité de leur demander si, par exemple, ce type de chose apparaissait devant eux, dans leur profession, est-ce qu'ils allaient savoir à qui s'adresser, de façon à échanger les informations, à mieux se connaitre, à jeter des ponts entre nous.

Cela a été très utile, comme nous le savons tous, il n'y a rien qui s'applique à tous les cas, mais dans ces domaines, dans ces régions, si cela était possible dans nos régions de le faire, ce serait très utile.

NICK WENBAN-SMITH: Merci, Pablo. Vous avez tout à fait raison. IL y a un écosystème où il y a des devoirs et des taches à réaliser et il est important de savoir à qui parler quand on a un problème et pour cela il faut des formations, travailler avec le secteur judiciaire, avec les procureurs, savoir comment aider une victime en cas de délits de ce type et savoir ce que nous

pouvons faire, dans le domaine de l'éducation aussi, quelles sont les ressources que nous pouvons fournir à ce secteur.

Il y a encore une question d'Allan McGILLIVRAY. Je ne vois pas cette question.

ALLAN MACGILLIVRAY : Ce n'est pas grave, je vais être rapide. Je suis du Canada. Quelques commentaires ou questions. D'abord je serais prudent concernant les conclusions que vous avez tirées de cette enquête, parce que des fois un échantillon ne représente pas toujours l'ensemble de la situation.

Ensuite, je suis d'accord avec le commentaire de Pablo.

À la diapositive 8, les données présentées, le nombre de ccTLD qui ne connaissent pas le taux d'utilisation malveillante du DNS, je dirais que c'est entre 25 et 30 %, c'est un chiffre inquiétant. C'est quelque chose qu'il faudrait essayer de mieux comprendre.

NICK WENBAN-SMITH: Oui, je suis tout à fait d'accord avec vous, ce n'est pas toujours des échantillons représentatifs de l'ensemble des ccTLD, peut-être qu'il y a d'autres histoires qu'il nous faudrait entendre. C'est pour cela que nous voulons continuer à travailler pour tirer davantage de conclusions.

En tout cas c'est une manière de comprendre la quantité d'utilisation malveillante qui existe, c'est vrai qu'on a du mal à répondre à cette question, on sait que les gens ont du mal à répondre quand ont

demande aux ccTLD quel est le nombre d'utilisations malveillantes du DNS trouvé dans leur travail au quotidien.

TATIANA TROPINA: Oui, d'ailleurs on a discuté de la méthodologie, du système d'échantillonnage dans le groupe et nous comprenons très bien que dans certaines mesures cet échantillonnage n'est pas représentatif. Mais pour nous, il est important de pouvoir constater l'existence de certaines tendances pour commencer à augmenter les compétences dans certains domaines, parce que si nous constatons la présence de brèches dans notre méthodologie, nous pouvons continuer à travailler.

En tout cas, pour le futur, nous pouvons vous dire qu'on a fait une analyse, on va continuer à faire cette analyse et on ne veut pas parvenir à certaines conclusions trop rapidement, comme comparer le taux d'utilisation malveillante et les prix réduits proposés par certains opérateurs. Voilà.

NICK WENBAN-SMITH: Nous sommes en retard, c'est pour cela que nous parlons trop vite.

Nous vous remercions pour votre participation, je remercie mes collègues pour la grande quantité de travail fourni ces dernières années.

CLAUDIA RUIZ : Merci, l'enregistrement est arrêté.

[FIN DE LA TRANSCRIPTION]