ICANN68 Forum virtuel de politiques — Séance sur les politiques d'At-Large : Utilisation malveillante du DNS : fixer un seuil acceptable
Mercredi 24 juin 2020 – 10 h à 11 h 30 MYT

[JONATHAN ZUCK] : Je pense que l'on devrait commencer.

MICHELLE DESMYTER : D'accord. Merci beaucoup. Bon. Bonjour ou bonsoir à tous. Bienvenue à la troisième journée de notre session At-Large du Forum virtuel de politiques ICANN68 ; nous sommes le mercredi 24 juin et il est 2 h UTC : « Utilisation malveillante du DNS : fixer un seuil acceptable ».

Je m'appelle Michelle DeSmyter. Je fais partie du personnel At-Large et je suis la responsable de la participation à distance pour cette séance. Veuillez noter que cette séance est enregistrée et suit les normes de conduite requises par l'ICANN.

Nous ne ferons pas d'appel nominal pendant la conférence ICANN68, mais nous noterons les présences pour toutes les séances. Pendant la séance, les questions ou commentaires soumis en chat ne seront lus à haute voix que s'ils sont soumis en anglais en utilisant le formulaire approprié, comme je l'ai fait remarquer dans le chat.

Je lirai les questions et commentaires à voix haute pendant le temps fixé à cet effet par le président ou le modérateur de cette séance. Pour poser votre question ou faire votre commentaire verbalement, veuillez lever la main. Lorsque votre tour arrive, nous activerons votre micro et vous pourrez prendre la parole. Veuillez alors indiquer votre nom pour l'enregistrement, ainsi que la langue que vous utiliserez si vous parlez une langue autre que l'anglais.

Veuillez noter que des services d'interprétation en français et en espagnol sont à votre disposition tout au long de cette séance. Pour bénéficier de l'interprétation, vous devrez télécharger l'application prévue à cet effet. Vous trouverez de plus amples informations dans les détails de la séance sur le programme de l'évènement, et des instructions seront affichées dans le chat.

Tous les détails ont également été publiés sur la page Wiki At-Large de l'ICANN68. Le lien aussi a été posté dans le chat. Nous vous rappelons amicalement de parler clairement et à une vitesse raisonnable afin de permettre une interprétation précise et nous vous demandons, encore une fois, d'indiquer votre nom chaque fois que vous prenez la parole. Sur ce, je cède la parole à Jonathan Zuck. Allez-y, s'il vous plait.

JONATHAN ZUCK : Merci Michelle. Je m'appelle Jonathan Zuck et je suis vice-président du Comité consultatif At-Large, spécialisé dans les politiques, et donc également coprésident du Groupe de travail At-Large sur les politiques consolidées.

At-Large est le principal défenseur des utilisateurs finaux individuels dans l'écosystème de l'Internet. À ce titre, il s'intéresse tout particulièrement au problème de l'utilisation malveillante du DNS. C'est donc un sujet sur lequel nous avons tenu un certain nombre de séances différentes au cours des dernières réunions, et il en va de même pour celle-ci.

Mais au cours de cette séance, ce que nous allons essayer de faire, c'est approfondir un point particulier plutôt que d'avoir un type de conversation plus généralisé. Et nous allons voir où ça nous mène. Pourriez-vous s'il vous plait afficher mes diapositives ? Très bien. Ils ne remplissent pas vraiment l'écran. Y aurait-il un moyen de les agrandir ? Je ne voudrais pas vous rendre la vie difficile ou quoi que ce soit de ce genre. Bon, je continue.

Donc, j'essaie toujours de ne pas avoir de liste à puces dans mes diapos. Voilà le premier point. Je pensais à une sorte de métaphore visuelle pour les discussions que nous avons eues sur la lutte contre l'utilisation malveillante du DNS.

De mon point de vue, ici, ce type en arrière-plan, c'est en quelque sorte un shérif. Et donc, il s'agit des gouvernements, des propriétaires de marques, des organismes de protection des consommateurs, etc. qui sont sur le point de s'affronter en duel avec… On dirait que quelqu'un est mis en muet. Sur le point d'avoir un duel avec des acteurs malveillants de l'écosystème du DNS. Et j'ose espérer qu'ils soient plus rapides à tirer. Diapo suivante.

Il y a cet autre problème : les membres de la communauté sont comme qui dirait en train de se promener entre nous, et il est très difficile de tirer sur le méchant sans pour autant toucher les habitants de la ville. Je pense que c'est une partie du défi que nous devons relever ; il est difficile de tirer sur le type qui se trouve de l'autre côté de la place quand de nombreuses personnes passent tout le temps entre nous. Diapo suivante.

Les utilisateurs finaux sont ceux qui souffrent en fin de compte dans cette bataille entre les différentes parties de l'écosystème de l'ICANN. Diapo suivante. Et nous savons qu'il reste des acteurs malveillants. Nous n'entendons que la voix des bons, mais il y a beaucoup de nouvelles tout récemment concernant GalComm et ce qui s'est passé avec un enregistrement de plus de 60 % de domaines malveillants auprès de ce bureau d'enregistrement. Diapo suivante.

Il y a donc la fameuse ligne de Star Trek selon laquelle il faut bien établir une limite quelque part. « C'est la limite à ne pas dépasser ». Voyons si ça va marcher ! Voilà. Diapo suivante.

Mais la question, bien sûr, et la question pour ce panel, est de savoir où tracer cette ligne. Diapo suivante. Ce que Graeme et Keith Drazek nous ont dit lors de la première séance du DNS, c'est que nous devons définir les caractéristiques des acteurs malveillants avant de pouvoir les combattre. Diapo suivante.

Alors, à quoi ressemblent ces caractéristiques que nous voudrions utiliser ? Quel genre d'indicateurs voulons-nous essayer d'utiliser pour

déterminer si nous avons affaire à un acteur malveillant ou simplement à quelqu'un avec qui nous devons travailler davantage ? S'agit-il d'un pourcentage des enregistrements malveillants par rapport au pourcentage du total des enregistrements ?

Parce que nous ne voulons pas punir les gens pour avoir réussi, mais plutôt obtenir une idée de l'ampleur de leur opération. S'agit-il du pourcentage de plaintes ? S'agit-il du délai de résolution moyen ? Portent-ils un chapeau noir ? Nous ne le savons pas vraiment. Mais nous voulons savoir quelles sont ces caractéristiques. Diapo suivante. Owen, je vois votre question sur la définition de l'utilisation malveillante, et aux fins de cette discussion nous allons la définir de façon très étroite. Drew va le faire, et il est le prochain intervenant.

Donc voilà, cela a été mon introduction. Je suis désolé, Michele, pour toute pensée sur [une quelconque responsabilité]. Il nous faudra en parler. Nous sommes honorés d'avoir dans notre panel David Conrad, vice-président sénior et directeur de la technologie de l'ICANN, et Drew Bagley, qui joue de nombreux rôles au sein de SecureDomains et de CrowdStrike. Donc, sans plus attendre, je voudrais passer le micro à Drew Bagley.

DREW BAGLEY : Merci, Jonathan. Êtes-vous en mesure de charger la présentation que j'ai envoyée ? Parfait. La voilà. Merci. Oui. Donc, j'aimerais aujourd'hui entamer la conversation en évoquant certaines des caractéristiques révélées par le travail que la communauté a réalisé. Elles nous

permettent de définir des indicateurs d'utilisation malveillante du DNS, notamment l'utilisation malveillante systémique dont parlait Jonathan et qui concerne certains de ces opérateurs comme celui qui a participé aux réunions de l'ICANN et, en général, ceux qui n'y participent pas. Diapo suivante, s'il vous plait.

Et donc, comme Jonathan et comme les divers représentants de la communauté, j'étais membre de l'équipe de révision de la CCT. Au moment où l'équipe de révision de la CCT réalisait son analyse et examinait les sauvegardes mises en œuvre dans le cadre du programme des nouveaux gTLD, ainsi que tous les problèmes recensés avant la mise en œuvre de ce programme, l'un des principaux problèmes que nous nous sommes attachés à mesurer était l'utilisation malveillante du DNS.

C'est pour cela que, dans le cadre de ce processus, l'ICANN a commandé l'Analyse statistique de l'utilisation malveillante du DNS dans les gTLD, aussi appelée SADAG. Cette étude a porté sur les nouveaux gTLD ainsi que sur les anciens, et a présenté une ventilation des taux d'utilisation malveillante par registre et bureau d'enregistrement.

En général - et pour plus d'informations sur la méthodologie, vous pouvez consulter le rapport lui-même ainsi que le rapport de l'équipe de révision de la CCT, les chercheurs se sont basés sur un horizon temporel de trois ans, puis utilisé plusieurs listes noires pour effectuer l'analyse. Diapo suivante, s'il vous plait.

Ils ont utilisé à cette fin la définition de l'utilisation malveillante du DNS que vous voyez ici, la même que celle utilisée par l'équipe de révision de la CCT, que nous avons appelée Menaces à la sécurité du DNS. Cette définition s'appuie sur des domaines communs et consensuels, tirés de la littérature citée dans notre rapport et concernant les domaines dans lesquels l'utilisation malveillante du DNS est hautement technique et liée à la cybersécurité, même si nous savons tous que l'utilisation malveillante du DNS peut, potentiellement, dépasser cela, selon le groupe auquel on s'adresse. Mais en général, c'est sur cela que nous nous concentrons, et c'est sur cela que la recherche elle-même a porté.

En ce qui concerne les parties auxquelles Jonathan a fait allusion, où l'utilisation malveillante se manifeste à un niveau élevé et où elle est concentrée, l'équipe de révision de la CCT, ainsi que cette étude particulière, ont découvert qu'il existe vraiment des zones particulières, certains TLD, ou certains bureaux d'enregistrement où l'utilisation malveillante peut représenter plus de 50 % du total des enregistrements.

Et donc, ces taux élevés d'utilisation malveillante du DNS ne sont apparemment ni aléatoires ni universels de sorte que chaque zone soit confrontée à ces mêmes taux. Il existe tout de même des endroits très particuliers et identifiables où le problème se pose avec acuité.

Et en plus de cela, il est également intéressant de noter que ces taux élevés d'utilisation malveillante peuvent se poursuivre sans relâche

pendant plusieurs trimestres, voire plusieurs années, sans qu'aucune mesure ne soit prise.

Et donc, en d'autres termes, un bureau d'enregistrement qui tirerait ses bénéfices d'un portefeuille constitué à plus de 50 % d'enregistrements malveillants serait toujours en activité avec ce portefeuille, et aucune mesure ne serait prise par le service de conformité de l'ICANN pour atténuer l'utilisation malveillante ou suspendre ce bureau si celui-ci ne l'atténuait pas lui-même. De même, ce bureau d'enregistrement ne prendrait aucune mesure à l'égard de ces titulaires de nom de domaine. Diapo suivante, s'il vous plait.

Ainsi, en plus de plusieurs autres recommandations visant l'utilisation malveillante, l'une des recommandations de l'équipe de révision de la CCT, la recommandation numéro 15, était axée sur cette utilisation malveillante systémique et continue. Et donc, alors que d'autres recommandations qui ont déjà été discutées précédemment… celles de l'ICANN se sont concentrées sur certaines mesures incitatives.

En fait, cette recommandation visait à garantir que ces opérateurs, dont les taux d'utilisation malveillante sont extrêmement élevés, et chez lesquels des utilisateurs sont pris pour cible et des violations de données sont perpétrées, ne puissent pas continuer à fonctionner sans que personne ne puisse intervenir pour y remédier.

Et donc, ici, la recommandation - toutes nos recommandations dans ce rapport étaient très longues, c'est pourquoi je n'ai pas tout mis sur la diapositive - essentiellement était que l'ICANN Org devrait s'assurer

que le service de la conformité de l'ICANN a le pouvoir de faire quelque chose à propos des taux élevés de menaces à la sécurité du DNS lorsque ceux-ci franchissent certains seuils.

Et bien que l'équipe de révision de la CCT n'ait pas été prescriptive dans la définition des seuils, elle les a suggérés. Les seuils suggérés étaient les suivants : si un seuil de 3 % des enregistrements est associé à des taux élevés d'utilisation malveillante, c'est là que le service de conformité devrait au moins lancer une enquête. Alors que si le seuil atteignait 10 %, la partie serait présumée être en violation des termes de son contrat. Et donc, cela a été basé sur les données sur les données qui nous ont été présentées dans l'étude. Diapo suivante, s'il vous plait. Diapo suivante, s'il vous plait.

[MICHELLE DESMYTER :] Une seconde.

DREW BAGLEY : D'accord. Aucun problème. Et donc, ces seuils ont été basés sur ce que nous avons observé avec ces taux extrêmement élevés. Donc voici quelques exemples. Lors de l'examen de ces données, il y avait donc deux bureaux d'enregistrement qui géraient des AlpNames particulièrement évidents. Ils ont fonctionné pendant des années avec ces taux extrêmement élevés d'utilisation malveillante.

Pour Nanjing, par exemple, 93 % des enregistrements de nouveaux gTLD qui leur étaient associés pendant une certaine période figuraient

en fait sur des listes noires. Finalement, Nanjing a été suspendu, mais pas seulement en raison de ce niveau d'utilisation malveillante.

C'était plutôt pour une série de choses. Et finalement, l'une des choses les plus incriminantes était qu'ils n'avaient pas payé les frais de l'ICANN. Et donc si l'on jette un coup d'œil rétrospectif sur les données, on s'aperçoit que Nanjing a fonctionné de cette façon pendant des années.

Pareillement, AlpNames a fonctionné jusqu'en 2019, date à laquelle il a finalement été suspendu. Mais il fonctionnait avec des taux d'utilisation malveillante extrêmement élevés, associés notamment à des TLD spécifiques tels que .science et .top.

Ce sont donc deux exemples clairs de parties qui ne participent pas aux réunions de l'ICANN. En général, ils ne jouent pas selon les règles. Et pourtant, ils s'en sortent impunément alors qu'ils constituent une source auprès de laquelle les cybercriminels peuvent enregistrer des noms de domaine pour les utiliser à toutes sortes de fins liées à cette définition que nous avons évoquée au début de cette session. Or, cela ne suffisait pas pour que quelqu'un fasse quoi que ce soit à ce sujet. Diapo suivante, s'il vous plait.

Voici donc certains des graphiques de l'étude SADAG qui mettent cela en évidence. On peut voir Nanjing, ici, tout en haut, avec un taux de 93,36 %, mais il y a plusieurs autres qui présentent des taux d'utilisation malveillante aussi élevés.

De même, quand vous vous rendez chez ces bureaux d'enregistrement qui s'occupent de zones particulières et qui présentent aussi des taux élevés d'utilisation malveillante, c'est là que vous pouvez vraiment voir ce chevauchement : si vous comptez enregistrer un nom de domaine à des fins malveillantes ou si vous voulez compromettre un nom de domaine légitimement enregistré, il y a une très forte corrélation entre certaines zones et certains bureaux d'enregistrement par rapport au succès qu'avaient ces cybercriminels et le fait de pouvoir maintenir impunément ces taux élevés d'enregistrement de noms de domaine. Diapo suivante, s'il vous plait.

Voici donc un exemple de zones pour lesquelles les registres avaient des noms de domaine avec… dont plus de 10 % des noms de domaine sont associés à des taux élevés d'utilisation malveillante. Ainsi, pour .science, la moitié des enregistrements de ce domaine étaient malveillants à ce stade-ci. Pareil pour .stream, près de la moitié.

C'est ainsi que ce concept de seuil est apparu au sein de l'équipe de révision de la CCT, en ce sens que si l'on se penche sur la question et que l'on pense aux parties contractantes, celles qui se battent contre les utilisations malveillantes et qui s'assurent que l'enregistrement de leurs noms de domaine est en grande majorité légitime au départ et qui, lorsque des noms de domaine sont compromis, prennent des mesures pour y remédier, que celles-ci ne figurent pas sur cette liste.

Cependant, lorsque des parties, qu'il s'agisse de registres ou de bureaux d'enregistrement, ne font apparemment rien ou ferment les

yeux et en tirent profit, vous vous retrouvez avec ces taux d'utilisation malveillante extrêmement élevés qui dépassent les 10 %. Diapo suivante, s'il vous plait.

Et voici donc d'autres données issues de l'étude qui mettent en évidence certains de ces éléments que je viens de passer en revue. On peut voir ici que dans le cas de certains noms de domaine, comme .download, le taux d'utilisation malveillante est très élevé, de sorte que 20 % de l'ensemble des enregistrements sont associés à une forme d'utilisation malveillante. C'est donc là le problème que la définition de seuils peut résoudre. Diapo suivante, s'il vous plait.

Donc, ce que ces données et ce que le travail de l'équipe de révision de la CCT dans ce domaine nous révèlent, c'est qu'il y a des parties qui sont soit utilisées par les cybercriminels soit spécifiquement ciblées ; par exemple, si vous avez enregistré légitimement des noms de domaine qui sont compromis par des cybercriminels.

Et pourtant, si ces parties ne sont pas incitées ou dissuadées de manière à ce qu'elles réagissent face à l'utilisation malveillante, celle-ci peut vraiment se perpétuer sur de très longues périodes, tandis que les gens continuent d'être pris pour cible par les mêmes sources, qu'il s'agisse de TLD particuliers ou de bureaux d'enregistrement particuliers.

Et tout ce concept est absolument incompatible avec la mission de l'ICANN concernant la protection de la sécurité et de la stabilité du DNS. Voilà pourquoi, au sein de l'équipe de révision de la CCT, nous

avons cherché un moyen de faire en sorte que le service de conformité de l'ICANN se penche sur les cas et lance une enquête lorsque des seuils élevés se présentent.

Et donc, parfois, lorsque le service de conformité de l'ICANN mène une telle enquête, il est possible de constater qu'une campagne active a été menée auprès d'un bureau d'enregistrement et que ce dernier a été lui-même pris pour cible.

Mais si vous avez des taux d'utilisation malveillante soutenus, aux alentours de 10 %, de même que si le bureau d'enregistrement est pris pour cible, l'enquête peut mettre cela en évidence.

Mais c'est là que, si vous fonctionnez avec des taux aussi élevés, il faut supposer que vous devriez avoir fait quelque chose pour les atténuer. Et si une partie ne fait rien à ce sujet, c'est là qu'elle aura du mal à rester accréditée. Au contraire, il serait nécessaire de recourir à la suspension de son contrat si l'utilisation malveillante n'est pas atténuée.

Et c'est là où la définition de seuils, en tant que communauté, constitue un outil important que nous pouvons utiliser à tout le moins pour nous attaquer à ces bureaux d'enregistrement particuliers qui sont utilisés et exploités par des cybercriminels à ces fins d'une manière incompatible avec la sécurité et la stabilité du DNS, mais aussi pour lesquels il s'agit vraiment d'un mauvais reflet du système des noms de domaine au regard de ce niveau concentré d'utilisation

malveillante, lorsque d'autres parties agissent de façon responsable et font quelque chose à ce sujet.

Et donc, pour inciter ces acteurs malveillants à agir de façon conforme et à atténuer l'utilisation malveillante, ou pour les amener à ne plus y participer, il est vraiment important de songer à cette recommandation de seuil.

L'équipe de révision de la CCT a plusieurs autres recommandations ayant trait à l'utilisation malveillante, mais je voulais juste me concentrer sur celle-ci aux fins de cette discussion, car nous discutons, en tant que communauté, de la manière d'aller de l'avant. Mais il est important de se rappeler qu'il y a vraiment beaucoup de données à l'appui de cette notion selon laquelle certains registres et bureaux d'enregistrement sont effectivement associés à des niveaux d'utilisation malveillante et dont nous n'entendons même pas parler par les parties qui se présentent ici aux réunions de l'ICANN.

Et donc, lorsque nous avons demandé à ce groupe intercommunautaire de l'équipe de révision de la CCT de se pencher sur la question, cela nous a beaucoup troublés et je pense que nous pouvons vraiment faire quelque chose pour y remédier. Sur ce, je retourne le micro.

JONATHAN ZUCK : Merci, Drew. Encore une fois, il semble que nous avons une discussion animée. J'espérais qu'elle le serait un peu moins, mais elle l'est à

nouveau dans le chat. David, je suppose que la parole est à vous, et pour finir ce sera le tour de Graeme. Allez-y, David.

DAVID CONRAD : D'accord. Merci. On m'a demandé de parler des informations dont nous disposons au sein de l'ICANN Org, et plus précisément au sein de l'OCTO, concernant l'utilisation malveillante du DNS. En ce moment, nous travaillons sur deux projets principaux. Le premier est le projet DAAR (DNS Abuse Activity Reporting), dont je suis sûr que tout le monde ici a entendu parler d'une manière ou d'une autre. Nous travaillons également sur un autre appelé Indicateurs de santé des technologies des identificateurs.

Les sources de données pour notre recherche interne utilisent des fichiers de zone du CZDS et des données de réputation provenant d'un ensemble de services de réputation du DNS. Nous avons documenté la méthodologie de sélection de ces services, dont la liste est fournie ici.

Les rapports du DAAR, actuellement, représentent un point dans le temps. Je crois qu'il s'agit du dernier jour du mois. En principe, nous prenons un instantané et en tirons un rapport. Et les ITHI sont des séries chronologiques qui sont basées sur des moyennes mensuelles. Diapo suivante, s'il vous plait.

Donc dans le rapport du DAAR que vous pouvez trouver sur le site de l'ICANN en suivant l'URL que j'ai fournie, vous trouverez une série de graphiques, un certain nombre de tableaux de formes diverses. L'un

des points qu'il convient probablement de souligner ici est qu'au fil du temps - et les rapports du DAAR ont, en gros, une fenêtre de six mois pour les utilisations malveillantes que nous suivons dans ces rapports - il semble que l'utilisation malveillante a, en général, diminué.

Vous avez évidemment des pics de temps en temps, chaque fois qu'une campagne est menée sous une forme ou une autre. Mais en observant les données présentées ici, vous verrez qu'avec le temps, les chiffres ont tendance à diminuer.

Je voudrais également faire remarquer que les gens, ici, trouvent parfois surprenante l'ampleur de l'utilisation malveillante. Si on regarde la figure 12, là, le pourcentage moyen d'utilisation malveillante par type de gTLD est d'environ 0,5 à 0,6 % du total des enregistrements. De même, si l'on regarde tout excepté le spam, on constate que ça ne dépasse pas 1 % des enregistrements.

Donc les chiffres, ici, dans l'ensemble, sont relativement faibles par rapport au nombre total d'enregistrements, et ce ne sont que les enregistrements qui apparaissent dans les fichiers de zone.

Il ne s'agit pas d'enregistrements qui sont faits ou détenus sans qu'ils soient renseignés dans les fichiers de zone, puisque le DAAR génère ses données à partir des informations publiées dans les fichiers de zone obtenus via le CZDS, le service centralisé de données de zone. Diapo suivante, s'il vous plait.

Nous fournissons également un certain nombre de diagrammes de points/corrélogrammes. Ils montrent tout, depuis le nombre brut de domaines résolus dans les gTLD jusqu'au nombre brut de menaces à la sécurité. Et vous pouvez remarquer, dans chacun d'eux, qu'il y a des cas où vous verrez des valeurs aberrantes.

Ainsi, dans le tableau des logiciels malveillants, en haut à droite, vous pouvez voir un point bleu, qui représente un nouveau gTLD, qui se démarque de tous les autres. J'ai en fait demandé à mon équipe, à Samaneh, la chercheuse qui en est la principale responsable, de trouver plus de renseignements là-dessus.

Elle m'a donné un aperçu des statistiques du DAAR, et il s'avère que c'est un unique… En fait, ce sont deux registres qui ont eu une quantité relativement élevée de logiciels malveillants, en ce sens qu'ils ont eu un nombre total d'enregistrements de sept, si je ne m'abuse, et l'un de ces enregistrements a en fait été utilisé pour la distribution de logiciels malveillants. Le pourcentage d'utilisation malveillante s'est donc révélé assez élevé.

De même, dans les domaines, le Botnet C&C, on observe de petits pics ici et là — autant d'indications d'aberrations qui méritent d'être explorées. Et c'est l'une des choses sur lesquelles mon équipe commence à se pencher. Nous identifions ces valeurs aberrantes, puis nous allons leur parler pour essayer de comprendre les raisons pour lesquelles elles sont ainsi.

Les résultats obtenus grâce à nos échanges avec les registres sont suffisamment satisfaisants. Car pour l'instant, le DAAR ne s'occupe que des données des registres et, plus précisément, des gTLD. Nous avons bien six ccTLD, mais les CC ne sont pas inclus dans ces statistiques. Pour l'instant, nous essayons de trouver la meilleure façon d'intégrer leurs informations dans les rapports du DAAR.

Mais nous allons auprès de ces registres et communiquons avec eux, et le résultat est satisfaisant. Si je comprends bien, les données présentées par Drew datent d'il y a trois ans. Et l'étude SADAG, je crois, a été publiée à cette même époque.

Et aujourd'hui, en consultant les statistiques que Samaneh a générées pour moi plus tôt ce matin, je n'ai vu aucun TLD qui selon les statistiques DAAR affiche plus de 20 % d'utilisation malveillante. Je crois qu'il y en a cinq qui présentent plus de 10 % d'utilisation malveillante, et cela inclut toutes les catégories d'utilisation malveillante que le DAAR examine, à savoir la commande et le contrôle de réseau zombie, la distribution de logiciels malveillants, l'hameçonnage et le spam.

En excluant le spam, ce dernier étant en quelque sorte une anomalie ennuyeuse en soi, vous obtiendrez des chiffres beaucoup moins faibles. Le plus élevé n'affiche actuellement que 1,4 % d'utilisation malveillante sans inclure le spam, et puis ça diminue assez rapidement. Diapo suivante, s'il vous plait.

L'OCTO utilise aussi comme source d'information les statistiques d'utilisation malveillante du DNS des ITHI, qui fait partie de la catégorie M2. Si vous allez sur ce site, vous trouverez un bel exemple de conception web des années 1990, ainsi que pas mal de données associées à l'utilisation malveillante du DNS.

Les statistiques y sont agrégées sur un mois, et les « hauts et bas » sont les hauts et bas historiques depuis que l'ITHI a été lancé.

Donc, une fois encore, il est important de noter que les chiffres de magnitude absolue sont en fait assez faibles, moins du dixième d'un pour cent dans la plupart des cas. Et le nombre total de TLD qui représentent 90 % des utilisations malveillantes est en fait assez faible, mais cela ne devrait pas être surprenant en raison de la concentration du marché.

En fait, un seul registre est responsable de plus de 50 % des utilisations malveillantes, mais je pense que personne ici ne pourrait affirmer que ce registre est coupable de quoi que ce soit, ou qu'il soit un acteur malveillant. Le fait est qu'il existe une corrélation très significative entre le nombre de domaines publiés et le nombre d'utilisations malveillantes.

On observe des valeurs aberrantes, comme je l'ai déjà mentionné, mais ce sont les… oh, le graphique a disparu. Pouvons-nous réafficher la diapo, s'il vous plait ? Mais en général, une des choses que nous essayons de comprendre au sein d'OCTO a trait à la définition des seuils évoqués : lesquels ont un sens réel et comment les appliquer

dans la pratique. La diapo suivante, s'il vous plait ? Ou n'importe laquelle. Ça y est, voilà. Non, mais on y est presque. Encore une diapo, je crois.

[MICHELLE DESMYTER :] En fait, c'était la dernière.

DAVID CONRAD : Ah ! C'est intéressant. D'accord. Eh bien, si vous allez sur le site web de l'ITHI, vous verrez un ensemble de séries chronologiques qui remontent jusqu'au tout début de l'ITHI. Là encore, la tendance générale que l'on observe est une diminution de l'utilisation malveillante au fil du temps.

Personnellement, je n'ai pas de données sur ce point, mais il me semble que c'est dû à l'attention accrue que diverses parties ont accordée à l'utilisation malveillante du DNS. Mais d'après ce que nous savons, le fait que l'utilisation malveillante du DNS diminue au fil du temps est une sorte de tendance de long terme. Cela dit, je redonne la parole à Jonathan.

JONATHAN ZUCK : Merci beaucoup, David. Je suppose que je vais poursuivre et donner la parole à Graeme. Il y a évidemment beaucoup de choses à discuter, au vu du chat et des présentations, et [nous avons perdu notre enregistrement]. Graeme, allez-y.

GRAEME BUNTON : Merci, Jonathan. Merci à ALAC et merci à vous Jonathan de m'avoir invité à participer à ce panel. On dirait que ça va être très controversé. Donc, je suis maintenant assez inquiet.

Permettez-moi de commencer par un remerciement pour la citation que vous avez partagée au début de cette présentation. Cette citation est toujours valable, et j'y reviendrai en fin d'exposé. Je n'ai pas de diapos. Je vais juste vous parler brièvement de certains points.

Donc, ce sujet relie de façon indissociable certaines des questions qui me préoccupent beaucoup, comme les données, l'élaboration de politiques basées sur les données et l'utilisation malveillante du DNS. Oh, on peut lire d'autres diapositives pendant que je fais ma présentation.

Peut-être que je vous dirai un petit peu sur mon propre contexte ; jusqu'à très récemment, je dirigeais le service des données au sein de Tucows et j'étais très impliqué dans la collecte et le traitement des données. Donc, il ne s'agit pas pour moi d'un point de vue occasionnel. C'est un sujet qui m'a déjà beaucoup occupé dans le passé.

Je vais donc commencer, peut-être, par quelques réflexions sur ce à quoi ressemblent les données vues de l'intérieur d'un bureau d'enregistrement, et cela vaut peut-être la peine d'être partagé. Il y a peut-être aussi un élément qui mérite d'être partagé ici, et il est

regrettable que le passage aux réunions virtuelles ait reporté cette session plénière.

Mais les parties contractantes ont essayé d'organiser une session avec la communauté de l'ICANN sur les réalités commerciales réelles de la gestion d'un registre et d'un bureau d'enregistrement, et sur ce à quoi cela ressemble ainsi que sur les aspects économiques d'une telle gestion.

Je pense que cela pourrait éclairer une grande partie de cette discussion, et j'encourage ceux qui ne comprennent pas vraiment les aspects économiques fonctionnels de ce secteur à faire quelques recherches et à réfléchir à ce sujet. Je n'en parlerai pas ici, mais il suffit de dire qu'il s'agit de l'enregistrement des domaines.

Du point de vue du bureau d'enregistrement, c'est une opération de grande envergure. Elle nécessite un volume important et les profits sont très minces, ce qui se répercute sur les données que nous collectons et sur la façon dont nous traitons les problèmes. Je ne voudrais pas pour autant me plaindre de notre position. Je pense que c'est juste une réalité commerciale qu'il nous faut reconnaitre.

Donc, là où je pense que cela influe sur les bureaux d'enregistrement en particulier, c'est que nous optimisons nos files d'attente d'utilisation malveillante pour un meilleur débit, et pour pouvoir fermer définitivement un dossier, et non pas pour collecter des statistiques sur ce qui se passe.

Reg, le directeur de la conformité chez Tucows, et moi en discutons tout le temps. Chez Tucows, nous adorons les données. Comme je l'ai déjà mentionné, c'est vraiment important pour moi. Nous aimerions commencer à personnaliser notre Zendesk, la plateforme que nous utilisons pour gérer notre file d'attente concernant les utilisations malveillantes, afin de pouvoir collecter plus de données sur les types de problèmes constatés, la façon de les résoudre et les résultats obtenus, car je pense que cela permettrait d'éclairer considérablement ce type de discussions.

Mais ce travail, pour nous, traine toujours loin derrière des travaux plus importants. Plus récemment, la réponse à l'utilisation malveillante liée à la COVID. Et si vous revenez à certaines des choses que Tucows a produites, vous trouverez d'excellents articles de blog sur les statistiques relatives aux demandes d'accès aux données des titulaires de nom de domaine, que j'encourage tout le monde à aller lire. C'est le fruit du travail de Reg, essentiellement, un travail fait à la main, et en collectant ces données.

Il est donc très difficile pour nous d'éclairer certaines de ces décisions de l'intérieur, lorsque ces données ne sont pas collectées uniquement au niveau de l'entreprise. Et je pense qu'il en va de même pour presque tous les bureaux d'enregistrement, et pour notre travail sur la COVID.

J'en ai parlé lors du webinaire de la Chambre des parties contractantes que nous avons organisé, je crois, le 11. Les statistiques

que j'ai présentées à cette occasion ont, une fois encore, été principalement recueillies à la main en saisissant des données dans des feuilles de calcul et en les révisant manuellement.

Tout cela pour dire que, au moment de collecter les données et d'y réfléchir, nous devons être exceptionnellement prudents dans notre façon de procéder, car les résultats finaux tout comme les implications pour les bureaux d'enregistrement et les parties contractantes dépendent grandement de la qualité de ces données.

Je ne veux pas parler trop longtemps, alors passons peut-être directement à l'idée des seuils. Donc, tout d'abord, en ce qui concerne la définition, je sais que nous ne voulons pas nous attarder sur cette conversation parce que nous l'avons déjà eue un milliard de fois.

Je répète ici que la Chambre des parties contractantes s'est mise d'accord, aussi formellement que possible, sur une définition de l'utilisation malveillante du DNS. Elle est très similaire à celle de la CCT, sauf que, à part le « spam de grand volume », elle précise « le spam qui est au service de logiciels malveillants, de réseaux zombies et d'hameçonnage », en bref.

Je voudrais encourager tout le monde à… Je suis sûr que nous pouvons trouver le lien correspondant. Elle est tirée du cadre de lutte contre l'utilisation malveillante du DNS. Merci, Sarah. Allez y jeter un coup d'œil. C'est à partir de cette base que nous aimerions travailler. C'est sur cette base que nous travaillons actuellement, les entreprises

qui retirent tous les jours des domaines pour utilisation malveillante du DNS.

Et dans une certaine mesure, c'est un point de repère, pas une limite. Chaque partie contractante est libre de l'adopter comme définition, c'est-à-dire comme point de repère, puis d'aller au-delà comme bon lui semble, et d'aborder les problèmes de la manière qui lui convient. Alors, commençons par là.

Une partie du problème, et une partie des préoccupations que je vois dans le chat et que les contractants éprouvent par rapport à l'idée des seuils… Et pour revenir à cette question de la qualité des données, ce qui à mon avis a vraiment été mis en évidence, c'est la qualité des listes que nous avons vues signaler des utilisations malveillantes.

Ces listes étaient, dans l'ensemble, terribles. Elles m'auraient fait déconnecter le site officiel de la réponse sud-africaine à la COVID, des sites web pour les hôpitaux. Les informations fournies étaient souvent de très mauvaise qualité, et nous devons être très prudents lorsque nous traitons ces flux.

D'autres personnes, plus proches que moi de l'utilisation malveillante du DNS du point de vue technique, vous diront que beaucoup de flux utilisés par les gens sont des signalements d'utilisation malveillante et ne sont pas nécessairement validés ou examinés. Et suspendre beaucoup de ces décisions très importantes sur la base de ces faits est, je pense, vraiment difficile.

Je pense qu'il y a aussi de réelles préoccupations quant aux conséquences des seuils. L'une de ces préoccupations, et je crois avoir vu Rubens y faire référence, est qu'ils pourraient être utilisés en quelque sorte comme arme contre les parties contractantes, ce qui est peut-être une préoccupation étrange, mais qui n'est pas hors du domaine du possible.

Et puis, il y a une autre… Je pense que ça s'appelle la loi de Goodhart. C'est qu'en définissant un seuil, on fixe ce qui deviendra une cible ; sans nécessairement motiver, vous avez déclaré : « vous pouvez être mauvais jusqu'à ce que vous ayez des ennuis ». Cela permet aux gens de comprendre exactement ce que cela signifie. Il y a peut-être une meilleure façon de s'attaquer à ce problème que poser ce genre de mesures incitatives.

Les seuils en général. Comment ferions-nous pour les faire respecter ? Je pense que les bureaux d'enregistrement tous azimuts - et je ne suis presque plus président, mais je pense pouvoir dire avec une certaine certitude raisonnable - préfèreraient de loin être créatifs avec les contrats que nous avons déjà et travailler avec le service de conformité de l'ICANN pour s'attaquer à ces acteurs malveillants de manière significative.

Le petit nombre d'acteurs malveillants qui me semblent avoir été… Et peut-être que la façon dont ils sont identifiés est une chose importante dont nous devrions parler. Mais j'estime que l'OCTO fait un

travail vraiment formidable et j'ai beaucoup apprécié cette présentation de David.

Cela fait chaud au cœur de voir que l'utilisation malveillante du DNS est en baisse. Mais comprendre comment l'OCTO et le service de la conformité peuvent commencer à collaborer pour trouver des moyens créatifs d'utiliser notre langage contractuel existant afin de faire la chasse aux acteurs malveillants, c'est susceptible de soulever quelques controverses.

Je serais vraiment curieux de savoir ce qu'en pense le service de conformité de l'ICANN. Je ne pense pas qu'ils soient là, mais c'est… Y a-t-il quelque chose ? Oh, je n'ai pas la référence devant moi. Je pense que c'est peut-être en vertu du 5.5.71, ou quelque chose qui s'en rapproche, que vous pouvez désaccréditer un bureau d'enregistrement pour impact significatif sur la sécurité et la stabilité du DNS — ou quelque chose du genre.

Y a-t-il des circonstances dans lesquelles cela s'appliquerait ? Je serais vraiment curieux de connaitre l'avis du service de la conformité sur ce que cela impliquerait pour eux. Ont-ils essayé un exemple hypothétique ?

Et donc, peut-être juste pour conclure, je dirais que nous devons faire très attention à la qualité des données que nous utilisons. Cela peut avoir un tel impact sur ce secteur, et les données, comme nous l'avons vu, peuvent être non seulement sensationnalistes, mais aussi complètement erronées.

Et là, je vais un peu vous importuner, Jonathan. En début de semaine, vous avez affiché une diapositive selon laquelle les domaines liés à la COVID étaient 50 % plus susceptibles d'être malveillants. Eh bien, 50 % plus susceptibles que quoi ?

Et si vous revenez à ce rapport, il portait sur une semaine de domaines qui a été effectivement saisie fin février, si je ne m'abuse, bien avant que nous ayons vu la majeure partie des enregistrements liés à la COVID, et il la comparait aux domaines que cette société particulière a eu l'occasion d'examiner pendant cette semaine-là.

Et si vous prenez cet « Oh, s'ils sont 50 % plus mauvais que les domaines en général » puis regardez la présentation de David sur les taux d'utilisation malveillante, vous trouverez que la probabilité d'une quelconque utilisation malveillante serait passée de… qu'était-ce ? D'environ 0,1 %, 0,01 %, à 0,015 %, ou 0,15 % ? Pour un petit bureau d'enregistrement, cela peut ne pas correspondre à un seul nom de domaine. Nous devons donc faire preuve d'une prudence extraordinaire dans la manière dont nous abordons ce problème.

Donc, pour en revenir à la citation que Jonathan Zuck vous a reprise de ma part - je pense qu'elle date de 2008 - je vais la répéter, c'est-à-dire… Je suppose que nous avons maintenant une définition, du moins celle de la CPH, que j'aimerais que nous utilisions, et je pense qu'il est important pour nous de le faire.

À présent, travaillons avec l'OCTO, qui fait un travail très intéressant en ce moment, sur la base de cette définition afin de vraiment définir

ou comprendre ce que font les acteurs malveillants et comment ils le font.

Précisons leurs attributs et leurs caractéristiques. Une fois que nous comprenons ce qu'ils font… Parce que je ne comprends pas. Je ne passe pas mes journées à chercher comment contourner les règles de conformité de l'ICANN ou comment… Je ne sais pas s'il y a vraiment un bon moyen de construire une entreprise sur des enregistrements malveillants, mais ce n'est pas une chose que j'essaie systématiquement de faire.

Donc, lorsque nous aurons parfaitement compris ces caractéristiques et ces attributs, nous pourrons déterminer les outils dont nous avons besoin pour y faire face, et cela pourrait consister en des interprétations créatives des contrats existants.

Il n'est pas impossible non plus qu'il s'agisse de nouvelles modifications contractuelles. Mais je ne pense pas que nous puissions vraiment dire de façon définitive ce à quoi cela va ressembler tant que nous n'avons pas mieux compris ce qui se passe réellement. Je crois que je vais terminer sur ce point. Merci.

JONATHAN ZUCK : Merci, Graeme. Je suis heureux qu'on m'importune à cause de mes données. Aucune question. Je suppose que ma question est la suivante… Je reviens à AlpNames, ou à certaines des autres parties

que Drew a mentionnées dans sa présentation, si longtemps après… Il semblait, à tous égards, évident qu'il s'agissait d'acteurs malveillants.

Il semblait impossible pour le service de la conformité d'agir à moins que ces personnes s'abstiennent de payer leurs factures, en principe, et cette impossibilité d'agir donne une mauvaise image de l'organisation. Je pense donc, moi aussi, que les contrats sont suffisamment vagues pour qu'il incombe presque à l'ICANN de donner une interprétation consultative du contrat et de préciser ses attentes à l'égard des parties contractantes.

Et je suppose que je pense aussi qu'un pourcentage soutenu de plaintes non traitées, ou sous quelque forme que ce soit, sur une certaine période, pourrait conduire à une enquête qui implique la vérification des informations, par opposition à un simple recours à une liste noire qui pourrait être basée sur des rapports ou autre chose de ce genre.

Donc, je suppose qu'il s'agit en partie d'une question de procédure qui pourrait conduire à une enquête plus approfondie. Mais même à la fin de cette enquête approfondie, nous devons nous assurer que nous disposons des outils nécessaires pour permettre au service de la conformité de prendre des mesures.

Donc, personne ne suggère que, d'une manière ou d'une autre, vous allez mettre au point un algorithme et désaccréditer automatiquement les bureaux d'enregistrement sur la base de ces données ou de quelque chose du genre.

Mais la question est de savoir s'il existe un flux de travail qui pourrait être mis en place et qui ne capturerait pas trop de dauphins dans le filet à thon, pour ainsi dire, et de trouver des moyens de s'attaquer à certains de ces acteurs malveillants.

Voilà ce que nous essayons de faire. Sur ce, je voudrais vous redonner la parole, Graeme. Je crois comprendre que cette notion de seuil n'est même pas nouvelle pour vous, et que vous avez déjà fait preuve de favoritisme à ce sujet par le passé, du moins à un moment donné.

GRAEME BUNTON : Je ne sais pas si j'aurais décrit ma position de cette façon.

JONATHAN ZUCK : Je n'essaie pas non plus de vous attirer des ennuis. C'est juste que je—

GRAEME BUNTON : Entendu.

JONATHAN ZUCK : -m'en rappelle vaguement ?

GRAEME BUNTON : Je m'excuse. Je suis terrible quand il s'agit de dire mon nom pour la transcription. Je ne suis pas contre l'idée en principe. Mais je pense que, dans la pratique, cela exigera énormément de travail. Et peut-

être qu'il faudra revenir un peu à la partie concernant la conformité, parce que je pense qu'elle vaut probablement la peine d'être mentionnée.

Quand nous réfléchissons à la manière d'être créatifs dans nos contrats et dans la conformité avec l'ICANN, il s'agit là d'un sujet récurrent au sein de l'équipe chargée de l'utilisation malveillante du DNS au sein du Groupe des représentants des bureaux d'enregistrement, à savoir comment travailler avec le service de la conformité. Pouvons-nous examiner nos contrats de sorte à suggérer au service des outils et des mécanismes auxquels nous serions favorables ? Et ces discussions n'en sont qu'à leurs débuts, mais j'espère que nous pourrons en tirer quelque chose à offrir à la communauté.

Mais nous sommes dans une sorte de drôle de situation en ce qui concerne le service de la conformité, c'est-à-dire que nous voulons qu'ils s'attaquent aux méchants. Ils donnent une mauvaise image de nous tous, ils accablent notre secteur, ils sont chiants. Désolé pour le langage grossier. Je suis surpris que ce soit la seule fois jusqu'à présent.

Et ils poussent les membres de la communauté ICANN à essayer d'atteindre des objectifs stratégiques qui, selon eux, visent les acteurs malveillants, mais qu'ils essaient en réalité d'appliquer à tout le monde, et ce n'est pas ce que nous voulons. Je ne pense pas que ce soit un secret, n'est-ce pas ?

Mais ce que nous ne voulons pas, c'est que la Conformité envoie aux bureaux d'enregistrement en permanence ce que quelqu'un a décrit comme des « contraventions de stationnement », en attaquant tout le monde dans l'espoir que les méchants trébuchent assez souvent pour qu'ils se retrouvent fauchés du fait de la règle en vigueur des trois infractions.

Parce que cela nous fait perdre notre temps, et que les bureaux d'enregistrement préfèreraient de loin répondre à des problèmes réels et concrets. Dans le passé, les requêtes d'inexactitude du WHOIS consommaient un temps [énorme] et ne valaient pratiquement rien.

Nous préférons de loin que la Conformité… Nous trouvons des moyens de recenser les problèmes matériels, de fond, et je pense que pour ce faire, il faudra réaliser un examen approfondi de nos contrats et avoir l'aide de la communauté. Merci.

JONATHAN ZUCK : David, Drew, est-ce que l'un d'entre vous souhaite rebondir sur les points qui ont été soulevés jusqu'à présent, à la fois par les autres intervenants et dans le chat, dans la mesure où vous avez pu le suivre ? Je vais céder la parole pour les questions.

DREW BAGLEY : Je vais commencer parce que je pense, en me basant sur une partie de ce que Graeme a dit, qu'il serait naturel pour David d'intervenir en

évoquant ce que le DAAR fait déjà, ou ne fait pas, ou cherche à faire, et ainsi de suite.

Je pense que, ici, vous avez vraiment beaucoup d'intérêts qui sont en harmonie. Car comme vous l'avez déclaré, Graeme, du point de vue de la réputation, il est clair qu'aucune des parties qui participent à l'ICANN ne voudrait être associée à d'autres comme AlpNames lorsqu'il s'agit, probablement, de quoi que ce soit, mais surtout lorsqu'il s'agit de discussions sur l'utilisation malveillante.

Je pense que c'est là donc que cette notion d'établissement de seuils est vraiment importante, malgré le fait que, comme vous l'avez dit, il faudra s'assurer que les données sont valides ; cet aspect des données est essentiel, et c'est là que j'aimerais que David nous en dise plus à ce sujet.

Mais ces données sont essentiellement utilisées en permanence dans le domaine de la sécurité des réseaux, en interne, lorsque les gens cherchent à savoir ce qu'ils vont bloquer de leurs propres réseaux. Elle est également utilisée par les chercheurs qui examinent ces données et les jugent suffisamment valables pour les utiliser à ces fins.

Donc l'existence de faux positifs n'indique pas nécessairement que toutes les données sont mauvaises, ou qu'un bureau d'enregistrement comme Nanjing, avec un taux d'enregistrement de 93 %, n'est pas associé à un niveau d'utilisation malveillante très élevé. Même si vous disiez : « D'accord, ces données ne sont pas toutes réelles », elles pourraient être associées à 50 % à celles que vous approuverez.

Et donc, dans tous les cas et sans aucun doute, ces choses peuvent toujours servir d'indicateurs. Et donc, en ce qui concerne la recommandation de la CCT, celle-ci a formulé une recommandation puis, dans les détails, a juste suggéré un seuil et une façon de faire fonctionner le processus.

Mais s'il existe un meilleur processus et un meilleur flux de travail, comme ceux dont parle Jonathan, il me semble que c'est ce que la communauté devrait absolument viser.

Parce que si la première indication ou la première chose qui se produit est que le service de la conformité de l'ICANN entame un dialogue, le simple fait qu'ils soient tenus d'engager ce dialogue avec une partie ayant atteint un certain seuil d'utilisation malveillante représente, à mon avis, une avancée formidable pour la communauté.

Et puis, on pourra faire évoluer les choses à partir de ce seuil. Une fois qu'un certain seuil est atteint sur une certaine période, et que le service de la conformité de l'ICANN ait effectué un certain nombre de tentatives pour travailler avec la partie concernée et résoudre le problème, peut-être que c'est là qu'il y aura d'autres mesures.

Et finalement, on arrive au point où, si l'on a affaire à une partie comme AlpNames ou Nanjing, elle pourrait être suspendue pour l'utilisation malveillante en soi plutôt qu'il ne faille rechercher d'autres motifs ou que cela prenne des années.

Et puis, en même temps, si l'on a une partie comme celles qui participent à l'ICANN, qui présente peut-être un pic passager d'utilisation malveillante ou quelque chose du genre, ou qui peut en fait dénoncer quelque chose avec les données utilisées, cela ne pose pas vraiment de problème.

Mais je pense que c'est une chose formidable, parce que vous pouvez toujours remédier à cette utilisation malveillante, en particulier lorsque nous parlons d'un bureau d'enregistrement ou même de zones entières, si vous trouvez cela problématique avec la zone ou avec le registre.

Je pense donc que le seuil en tant qu'outil est très important et qu'il pourrait être utile, et je pense que les incitatifs sont alignés. Et évidemment, il s'agit de parfaire les détails.

Mais je pense que l'objectif global remonte à l'un des objectifs définis au début du nouveau programme gTLD, même si la discussion actuelle est plus générale, qui était de faire en sorte qu'il n'y ait pas d'acteur malveillant qui exploite des registres ; et l'on ne voudrait pas non plus que des acteurs malveillants exploitent des bureaux d'enregistrement.

Il me semble vraiment important – et je veux savoir ce qu'en pense David – d'avoir les bonnes données, mais aussi de ne pas ignorer les données qui sont bonnes dans l'ensemble simplement parce qu'elles présentent de faux positifs, ce qui devrait être pris en compte, bien sûr.

Et puis aussi le flux de travail lui-même. Il faudra le prendre en compte. On pourrait intégrer des sauvegardes dans le flux de travail, mais je pense qu'en tant que communauté nous avons vraiment beaucoup de choses que nous pouvons faire à ce sujet. Et donc, David, j'aimerais connaitre votre avis, parce que je pense que le DAAR peut constituer un outil important en ce sens.

DAVID CONRAD : Entendu. L'un des défis à relever, compte tenu des ensembles de données dont nous disposons actuellement, consiste à essayer de déterminer ce qui est réellement pertinent. Donc en prenant par exemple les suggestions de seuil de la CCT, et au regard des données instantanées du DAAR que j'ai obtenues ce matin, il y aurait 11 domaines de premier niveau ayant dépassé le seuil fixé à 3 %.

Ces 11 domaines représentent au total environ 10-11 % de tous les enregistrements malveillants actuellement figurant dans le DAAR. Donc au total environ 622 000 enregistrements malveillants. Ce qui veut dire que le total dont nous parlons ici est relativement faible. Il est de l'ordre de 70 000 à 80 000 domaines malveillants.

Et l'une des vraies difficultés réside dans le fait que le spam, étant si fréquemment utilisé, fausse tous les pourcentages. Il fausse toutes les statistiques que nous recueillons. Alors vous dites : « Bon, d'accord. Ignorons le spam. Concentrons-nous sur toutes les utilisations malveillantes, donc l'hameçonnage, les logiciels malveillants, le commandement et le contrôle, qui n'incluent pas le spam ».

Nous serons face à un problème différent, car personne n'atteindrait le seuil de 3 %. Dans les statistiques existantes, ce chiffre atteint 1,4 %. Bon. Vous abaissez alors le seuil, ce qui soulèvera différentes questions.

Et cela revient à supposer que vous ne voulez pas vraiment vous soucier des domaines dont les enregistrements malveillants ne dépassent pas un certain nombre, comme par exemple 1 000 ou quelque chose du genre, parce que vous ne voulez pas vous en prendre aux tout petits registres qui ont un ou deux enregistrements qui font exploser leurs statistiques.

Je pense que c'est en partie pour cette raison que nous avons essayé de trouver les valeurs aberrantes… Puis, nous avons essayé de travailler avec elles pour comprendre, A, pourquoi elles sont aberrantes, et les aider, si possible, dans l'atténuation. S'ils choisissent de ne pas atténuer, cela constitue en soi une information intéressante qui peut alimenter les discussions communautaires.

S'il y a des acteurs qui savent qu'une certaine approche commerciale qu'ils adoptent les amène à devenir un foyer ou une cible pour tous les titulaires malveillants, alors peut-être que la communauté peut entreprendre quelque chose de sorte à explorer cette piste. Peut-être que cette pratique commerciale particulière n'est pas viable si vous voulez réellement avoir un écosystème sain du DNS.

Je suis donc un peu réticent à accepter le modèle des seuils arbitraires, juste des chiffres fixes, parce qu'il existe tellement de

variables qui jouent dans ce qui est réellement une utilisation malveillante et dans la façon dont une pareille utilisation affecte les registres/les bureaux d'enregistrement.

La seule réalité est qu'il y a un certain nombre de titulaires malveillants, et ils profitent de tous les mécanismes possibles pour pouvoir être malveillants, pour se remplir rapidement les poches, comme on le disait autrefois.

Et j'ai eu l'impression que ces titulaires malveillants sont un ensemble relativement stable d'individus qui se trouvent à rebondir entre les registres et les bureaux d'enregistrement lorsque ces derniers correspondent à leur modèle commercial malveillant particulier.

Il n'est généralement pas question de cibler un registre ou un bureau d'enregistrement particulier, bien que cela puisse arriver. Il y a eu des cas où il apparait clairement que certains registres ou bureaux d'enregistrement sont malveillants. Ceux auxquels je pense n'existent plus.

Mais il faut bien admettre que certaines personnes sont en quelque sorte en train de passer d'un endroit à l'autre, de faire des choses répréhensibles, et qu'il faut trouver un moyen de rendre moins tentantes ces choses répréhensibles ; or, ce n'est pas une fonction intrinsèque des seuils. C'est la fonction des politiques et des processus par lesquels les entreprises fonctionnent. Et pour être clair, cette opinion m'appartient et ne reflète en aucun cas la position de l'ICANN.

JONATHAN ZUCK : Merci David. Nous avons quelques questions à poser. Donc, si vous en voyez qui vous sont adressées dans la partie questions-réponses... Et Drew et David, je pense que certaines vous sont adressées. Je peux les lire, ou vous pouvez taper les réponses, peu importe. Nous avons Brian Cimbolic dans la file d'attente qui a la main levée. Il peut maintenant désactiver son muet. J'ignore s'il est toujours en muet. Allez-y, Brian.

BRIAN CIMBOLIC : Bonjour à tous. J'espère que vous m'entendez bien. Merci beaucoup. Je pense que cette séance fait vraiment réfléchir. La seule chose que je veuille dire… Et ici au PIR, nous sommes très engagés dans la lutte contre l'utilisation malveillante, l'utilisation malveillante du DNS, sous toutes ses formes. La seule chose que je dirais, c'est que les fournisseurs tiers, même bien intentionnés, peuvent souvent conduire à de faux positifs assez importants.

Ainsi, si vous suivez les taux d'utilisation malveillante d'un TLD mois après mois, vous pouvez constater une multiplication par deux, trois, quatre ou cinq du « pourcentage d'utilisation malveillante », sans qu'il y ait en fait d'augmentation sous-jacente de l'utilisation malveillante, comme des noms de domaine bruts et malveillants.

On ne sait donc pas grand-chose sur le fonctionnement des fournisseurs tiers. Il y a peu de transparence. Et vous finirez par constater des pics importants de pourcentages dans tous les

domaines sans augmentation sous-jacente de l'utilisation malveillante.

Cela a également été le cas avec le pic des enregistrements COVID où, pour .org, par exemple, nous avons vu 14 700 enregistrements de noms de domaine liés à des coronavirus ou à la COVID. Au total, 13 d'entre eux étaient passibles de poursuites pour utilisation malveillante du DNS ou d'un contenu de site web, limitée strictement à la vente de faux remèdes ou de faux vaccins. C'est donc moins d'un dixième d'un pour cent.

Et puis, on nous a remis des listes où, en principe, tous les noms de domaine liés à la COVID ou à des coronavirus avaient fait l'objet « d'enregistrements frauduleux », y compris certains noms de domaine enregistrés par les Nations Unies qui servaient vraiment à des fins légitimes.

Je veux donc dire que, dans la mesure où quelqu'un puise dans des données de tiers, ce que je comprends puisque c'est en quelque sorte tout ce qui existe, nous devons être très prudents dans le choix de ce que nous puisons et dans notre compréhension des avantages et des failles potentielles de ces listes.

JONATHAN ZUCK : Merci Brian. Cet aspect des listes a été largement évoqué dans toutes les séances de cette semaine. Et donc, peut-être que nous devrions

travailler avec certains de ces créateurs de listes pour que le résultat de leur travail soit notamment plus granulaire.

Une conversation a eu lieu dans le chat. Je pense que Steve DelBianco avait souligné, plus clairement que je ne voulais le faire, qu'il n'y a jamais eu le sentiment qu'il y aurait une sorte de désaccréditation automatique.

Comme l'a dit Jeff Neuman, ce ne devrait pas être là l'objectif, certes. Mais lorsque les ressources du service de conformité sont limitées, on pourrait se servir d'un pourcentage élevé et persistant d'utilisation malveillante pour entamer des conversations, comme l'a mentionné David…

Ensuite, si ces conversations ne mènent nulle part, potentiellement être capable de faire sa propre enquête, mais aussi disposer des moyens de désaccréditer un bureau d'enregistrement au cas où ce dernier échoue ou est réticent à résoudre le problème indiqué par certaines de ces données.

Donc, là encore, je ne pense pas que ces données devraient déclencher automatiquement quoi que ce soit, mais elles pourraient servir de guide à bien des égards. Brian, avez-vous encore levé la main ?

BRIAN CIMBOLIC : Excusez-moi, non. Je suis désolé. Merci.

JONATHAN ZUCK : Merci. Donc, Fabricio a écrit dans le chat : « [inaudible] mesures constituent un bon début, c'est-à-dire le Cadre de lutte contre l'utilisation malveillante des domaines. Mais y aurait-il un moyen de renforcer la transparence de sorte que la communauté sache que ces mesures fonctionnent et que les signataires respectent les engagements qu'ils ont pris ? »

Merci, Fabricio, de votre question. Il me semble que Graeme devrait probablement répondre à cette question. Mais ce que nous essayions de faire, entre autres, était de déterminer s'il existait des mesures objectives, ici, plutôt que d'essayer de dicter aux parties contractantes comment faire leur travail, parce que c'est ce dernier point qui a suscité beaucoup de rejet.

La révision de la CCT a permis de formuler un grand nombre de recommandations très spécifiques. Nous nous sommes entretenus sur l'enregistrement en masse, par exemple, et sur certains des problèmes connexes.

Donc ce que j'essayais vraiment de faire pendant cette séance, c'était de voir s'il y avait un moyen de prendre du recul par rapport aux recommandations pratiques, ou aux règlements, si vous le permettez, et de rechercher les mesures objectives que l'on pourrait utiliser, en laissant les registres et les bureaux d'enregistrement résoudre eux-mêmes les problèmes auxquels ils sont confrontés.

C'était donc l'objectif. Mais Graeme, voulez-vous répondre à la question de Fabricio sur la conformité vis-à-vis du cadre ? Si celui-ci devient un nouveau SEC ou quelque chose du genre, une sorte d'autorégulation, y a-t-il un moyen ou des paramètres permettant de vérifier que ces cadres sont effectivement respectés juste parce que quelqu'un les a signés ? Merci, Graeme. Je vous laisse la parole.

GRAEME BUNTON : Merci, Jonathan. Je ne suis pas sûr de pouvoir parler au nom de tous les signataires du cadre, mais je sais que Brian participe à l'appel, donc il pourrait dire ce qu'il en pense aussi. Actuellement, nous ne disposons pas d'une équipe chargée de faire respecter ce cadre volontaire.

Quand les gens nous disent « Je veux m'inscrire », nous leur faisons savoir assez clairement que ce choix, à notre avis, devrait être sérieux. Il ne s'agit pas pour nous de présenter une image flatteuse tout simplement. Et nous le disons assez clairement en espérant de tout cœur que les gens respectent ce cadre avec sincérité.

Si une partie quelconque en profitait pour se créer une image flatteuse et, essentiellement, abusait de la bonne volonté de ce groupe et du bon travail que ce dernier a accompli en y apposant son nom sans toutefois agir en conséquence, serais-je contrarié si elle était rappelée à l'ordre d'une manière ou d'une autre ?

Et puisque je ne collecte pas les données sur ce que font les autres, ce ne sera pas à moi d'agir. Je dirais simplement que je n'en aurais pas le cœur brisé. Merci.

JONATHAN ZUCK : Merci, Graeme. Une certaine réticence a toujours existé, et il s'agit de trouver le juste équilibre. Le service de la conformité a toujours été réticent à faire ce que les gens appellent la « mise au pilori », ou à nommer les parties impliquées dans des activités répréhensibles, etc.

Et donc, il y a une complexité associée à cela, car, comme Jeff l'a mentionné, le but n'est pas de désaccréditer qui que ce soit, mais de modifier les comportements. Donc on peut sans mal comprendre qu'il y ait une hésitation à agir en ce sens.

Et la question est de savoir où se situe le seuil à partir duquel vous agissez, et les informations deviennent alors disponibles pour que les gens puissent décider avec qui traiter. Fabricio, je suppose que vous avez quelque chose à ajouter. Allez-y. Fabricio, je ne vous entends pas. Je ne sais pas si vous avez pu désactiver le muet. Oui. Alors, maintenant vous pouvez. Allez-y.

[FABRICIO :] Vous m'entendez ? Vous m'entendez maintenant ? Parfait. Bonjour. Merci. Je tiens donc à dire que, à mon avis, cette séance a été l'une des plus productives auxquelles j'ai assisté jusqu'à présent. Je voudrais remercier, en particulier, Graeme, donc me joindre ici à l'équipe de

meneurs de claque de Graeme. J'ai toujours apprécié sa franchise lors des conversations que nous tenons.

J'ai donc pensé qu'il serait utile de poser une question sur la transparence dans le sillage de la discussion. Je pense que la transparence contribuerait grandement à ce que la communauté accorde une crédibilité aux engagements pris.

Et la raison pour laquelle je voudrais rebondir sur ce point est que j'ai posté dans le chat, ici, une lettre de 2008 dans laquelle nous avions initié une communication avec Jamie Hedlund de la Conformité. Cette initiative a pris l'acronyme ICWP, Groupe de travail indépendant sur la conformité.

En fait, si vous preniez quelques minutes pour lire la lettre initiale, et n'hésitez pas à lire les autres, vous verrez que nous avons tenu cette même conversation sur les approches proactives, basées sur les données : la transparence, l'accord général sur la teneur des données, le fait de veiller à jeter le filet assez loin pour attraper des parties comme Alpnames, dont le comportement est scandaleux aux yeux de tout le monde, sans toutefois attraper accidentellement des personnes qui présentent quelques variations dans les enregistrements, etc.

Et je voudrais revenir, en particulier, sur une conversation. Après cette lettre, je me suis réuni autour d'une table avec Graeme, Brian et beaucoup d'autres personnes de cette liste.

Je pense que nous avons eu une conversation de plus d'un an sur la manière dont nous pourrions organiser ou proposer à la communauté une discussion sur les bons déclencheurs et la façon la plus judicieuse de tendre nos filets en veillant à ce que le fardeau ne retombe pas toujours sur des parties bien intentionnées qui investissent de l'argent pour freiner l'utilisation malveillante du DNS, et qui sont constamment dépeintes sous un mauvais jour par les vilains Alpnames du monde.

Et donc, je me demande… Nous avons eu des conversations vraiment géniales et productives. Avant Marrakech, nous en étions au point où les gens disaient : « Oui, il semble que nous pourrions commencer à nous pencher sur les seuils et à comprendre ce que nous essayons de cibler pour ne pas entretenir des dialogues de sourds ».

Et puis, cette conversation s'est en quelque sorte dissipée ; elle a disparu. On dirait qu'elle refait surface. Et je me demande simplement s'il y aurait un moyen de revenir dans cette conversation au point où les parties contractantes établissent leurs propres normes, dont le respect est garanti à la communauté, et où nous avons tous confiance dans les mêmes rapports, la transparence des données de l'ICANN, etc.

Parce que, malheureusement, ce que je continue de voir, c'est que beaucoup de gens font de sérieux efforts - Graeme et son groupe, entre autres, mènent en quelque sorte la charge en la matière - et qu'il

y a de nombreux membres de la communauté qui veulent que quelque chose se passe.

Et chaque fois que nous nous rendons auprès d'ICANN Org, celle-ci fait tout simplement retomber la pression et refile la responsabilité aux bureaux d'enregistrement. Ils n'assument aucune responsabilité et fournissent beaucoup de données qu'ils ne sont toutefois pas prêts à prendre en charge. Ils refusent de s'engager de quelque manière que ce soit. C'est toujours le problème d'autrui.

Et je me demande, puisque c'est notre problème, ne pourrions-nous pas tous discuter et trouver des solutions que nous pourrions appliquer, faire en sorte que ce soit transparent en tant que communauté, des solutions dont nous pourrions tous convenir sur la base des données, etc. ? Parce que c'est sur cela qu'a porté la conversation pendant un an, puis elle s'est éteinte, comme je l'ai dit.

Donc, plutôt que de revisiter 2018 et 2020, et de tenir de nouveau cette même conversation en 2024, quand quelque chose d'autre se présentera, pouvons-nous juste reprendre le fil de cette conversation et trouver des solutions que la communauté puisse examiner à fond et dont elle pourrait convenir ?

GRAEME BUNTON : Je vais rapidement intervenir. Je suis d'accord, ces conversations étaient bonnes. Je vois Crystal Ondo dans le chat disant que certaines de ces conversations ont été organisées par Bryan Schilling, et peut-

être serait-il bon de voir certaines d'entre elles refaire surface. Je ne crois pas que ce soit une mauvaise idée.

Commençons donc. Réfléchissons à ces solutions créatives pour le service de conformité. Voyons si nous pouvons faire avancer les choses de manière significative, et pas seulement à la manière de l'ICANN : avoir des conversations interminables sur les mêmes sujets. Merci.

JONATHAN ZUCK : Merci, Graeme. Merci, Fabricio. Michele, le tour est à vous.

MICHELE NEYLON : Vous m'entendez bien ?

JONATHAN ZUCK : Oui.

MICHELE NEYLON : Parfait. Bonjour. J'ai juste quelques commentaires. On a donc beaucoup parlé du cadre de lutte contre l'utilisation malveillante du DNS, qu'un assez grand nombre d'entre nous, qui représentent, si je ne m'abuse, plus de 90 % des enregistrements gTLD dans le monde, ont signé. Et je pense que c'est là qu'il y a une sorte de confusion entre les concepts à laquelle les gens doivent vraiment faire attention.

Les bureaux d'enregistrement et les registres sont des entreprises. Si nous fonctionnons, et si nous sommes en mesure de fonctionner, évidemment, c'est en vendant des produits et des services et en gagnant de l'argent, parce que le capitalisme n'est pas une si mauvaise chose.

Et les sociétés et entreprises impliquées dans des pratiques douteuses finissent par être poussées en dehors du système, à bien des égards.

Or, dans l'espace ICANN, il existe semble-t-il cette sorte de croyance que vous pouvez nous battre à plate couture avec nos contrats, ce qui, à mon avis, serait ce que certains considèrent comme probablement la « façon de régler les choses », alors que beaucoup d'entre nous estiment que ce n'est pas vraiment ainsi que les choses devraient fonctionner.

C'est pourquoi, je pense, certains d'entre nous sont en désaccord avec la façon dont le cadre de lutte contre l'utilisation malveillante, que nous avons volontairement signé, est considéré. Parce que vous nous demandez de nous soumettre à une sorte de fonction de conformité concernant quelque chose que nous avons signé volontairement et en toute bonne foi.

Alors que, en réalité, pour beaucoup d'entre nous, comme l'ont souligné Brian et Graeme je pense, le cadre que nous avons accepté n'est qu'une base de référence. Beaucoup d'entre nous font beaucoup plus, et volontairement.

Nous le faisons par le biais de nos conditions de service. Nous le faisons par le biais de nos politiques d'utilisation acceptable. Nous faisons des choses qui nous donnent des résultats et qui fonctionnent pour nos entreprises, avec lesquelles nous sommes à l'aise. Et nous assumerons le risque juridique si nous estimons que ces choses nous conviennent.

Mais ce choix nous appartient. C'est quelque chose que nous faisons et, au fil du temps et des circonstances, nous adaptons nos méthodes à notre propre gré. Alors que, dans l'espace ICANN, vous parlez de contrats qui ne peuvent et ne doivent pas être constamment modifiés et transformés afin d'être adaptés au gout du jour.

Il faut donc faire très attention à la façon d'encadrer une grande partie de cette discussion. Et je partage beaucoup des préoccupations exprimées par d'autres au sujet de certaines listes noires et autres sources de données, car celles-ci ne sont pas toutes égales.

Et le simple fait qu'un nom de domaine soit sur une liste noire ne signifie rien en réalité, car certains fournisseurs de listes noires, littéralement, ajouteront des choses sur une liste parce qu'ils sont tombés du lit le matin ou étaient de mauvaise humeur.

Ou dans certains cas, ils essaieront, en fait, de soutirer de l'argent à la fois aux bureaux d'enregistrement, aux registres et aux titulaires qui souhaiteraient retirer leurs domaines de ces listes noires. Donc, je pense que beaucoup de ces conversations pourraient avoir lieu, et je pense que certains d'entre nous seront ravis d'y contribuer.

Mais il faut que ce soit une conversation, pas ce genre de bêtises hyperboliques que nous avons vues si souvent ces derniers mois, où les gens prennent une étude mal écrite ou un article mal documenté et le brandissent comme s'il était, en quelque sorte, basé sur des faits, ce qui, dans de nombreux cas, n'est pas vrai.

Et ceux d'entre nous qui travaillent au quotidien dans cet espace peuvent signaler beaucoup de failles et de suppositions extrêmement dangereuses contenues dans un grand nombre de ces « rapports » et « études ».

Faites extrêmement attention à la façon dont cela est encadré. Un vœu ne se fait pas à la légère. Parce qu'il est très facile de faire basculer les choses et se retrouver dans une situation où les acteurs malveillants, terme que je déteste, sont capables de contourner les choses, alors que beaucoup d'entreprises qui ont simplement atterri un mauvais client finissent par en pâtir. Merci.

JONATHAN ZUCK : Merci, Michele. Je pense que ce sont d'excellentes contributions. En fait, c'était en quelque sorte l'idée derrière cette séance, de ne pas essayer de dicter les pratiques des registres et des bureaux d'enregistrement, mais, au contraire, de se contenter d'observer les résultats.

Les problèmes liés aux données sont évidemment extrêmement importants, et nous devons trouver la meilleure façon de les résoudre.

Mais s'il s'agit d'une indication pour faciliter l'enquête de manière plus directe, ou quelque chose de ce genre, c'est peut-être la voie à suivre.

Mais une fois que cela est établi, le problème devient aussi de savoir si les contrats ont une base suffisante. Et il me semble que oui, et, si je l'ai bien entendu, il me semble que Graeme le croit aussi — qu'une fois que vous avez vraiment une idée de ce que sont les pratiques commerciales, le contrat actuel fournir une base assez solide pour aller de l'avant.

Peut-être faudrait-il simplement essayer. Je ne possède pas la réponse, mais c'est justement l'idée : arrêter de pinailler dans un tas de pratiques et vouloir les intégrer au contrat, mais plutôt interpréter le contrat de manière à garder les choses bien en main, pour ainsi dire. Je pense que c'est au tour de Fabricio. L'ordre est bon il me semble alors allez-y, s'il vous plait.

[FABRICIO :] Bonjour. Oui, je voulais juste faire un suivi très rapide, Jonathan, et vous m'avez ouvert la porte. Oui, en fait, c'était le point essentiel des conversations que nous avons eues pendant plus d'un an, à savoir essayer de trouver des déclencheurs très importants qui permettraient au service de la conformité d'intervenir.

Je vais le dire, sans vouloir pour autant mettre de mots dans la bouche de Jamie. Il semble cependant que le service de la conformité ne cessait de dire : « Nous aimerions vraiment pouvoir agir, mais on

nous dit que nous ne pouvons pas », ou « nous ne voyons pas de position », flanqués à gauche et à droite de membres comme moi de l'IPC et de membres de la Chambre des parties contractantes qui regardent Jamie répondre : « Nous voyons bien que certains éléments du contrat vous permettent d'intervenir. Qu'est-ce qui vous retient ? »

Et ce concept de déclencheur, de seuil… Je ne veux pas le convertir en arme, mais ce concept du moment où la non-conformité est si flagrante et ne fait aucun doute, il devrait au moins déclencher une enquête ou quelque chose dans le sens où vont les conversations.

Et donc, oui, ajoutez mon nom à la liste de ceux qui sont d'accord avec vous. Et ce sur quoi vous disiez penser que Graeme était d'accord, je vais dire carrément que je suis d'accord là-dessus aussi, parce que je pense que c'est ce qui manque, au lieu d'utiliser ces données comme déclencheur lorsque c'est vraiment évident.

Ce que j'entends les parties contractantes dire, et ce que nous constatons, c'est qu'au lieu de cela, le groupe de la conformité se lance dans ce système de solution de facilité, où il se contente de courir en tous sens et de s'en prendre à tout le monde pour des choses qui n'ont pas vraiment d'importance, et c'est une énorme perte de temps, d'argent et d'efforts pour les parties contractantes.

Cela ne sert en rien la communauté et les gens comme nous qui demandent de réduire les niveaux d'utilisation malveillante, et cet effort pourrait aller ailleurs pour démanteler des parties comme Alpnames, comme vous l'avez justement souligné. Je pense que la

lettre que j'ai publiée cite le rapport du DAAR dont nous avons entendu Conrad parler pendant toute cette séance.

On leur a noté plus de 38 %, je pense, des utilisations malveillantes provenant de cette petite ile, et pourtant ils ont essentiellement fonctionné jusqu'à ce qu'ils ne puissent plus payer leurs factures, non pas parce que le service de la conformité est intervenu.

Et lorsque nous avons demandé pourquoi celui-ci n'avait rien fait, c'était parce qu'ils s'étaient justement livrés à la pratique que les parties contractantes ne peuvent pas supporter, qui consiste à tirer au hasard de petites contraventions de conformité, puis à fermer les contraventions lorsqu'on leur répondait « Eh bien, ce nom de domaine a maintenant disparu », au lieu de s'attaquer au problème de fond en se basant sur les données, et celui-ci subsistera. C'est donc pour cela qu'une approche proactive, basée sur des données et comportant un certain niveau de seuils évidents, rendrait un bon service à toutes les personnes concernées.

JONATHAN ZUCK : Thanks, Fabricio. Je suppose que je n'ai pas regardé l'onglet des panélistes, et donc je ne sais pas comment procéder dans l'ordre. Graeme, vous levez aussi la main ?

GRAEME BUNTON : Oui.

JONATHAN ZUCK : OK, allez-y.

GRAEME BUNTON : Je serai très bref. Merci. Juste un petit mot sur les contrats. Je veux vraiment qu'il y ait quelque chose dans les contrats actuels. Ce serait ma préférence. Et pour ce qui est du contexte, les négociations contractuelles avec les parties contractantes sont des affaires longues et couteuses qui s'éternisent.

Je pense que la série de 2013, et c'est un peu avant mon temps, a pris environ 18 mois. Je pense que des négociations axées sur l'utilisation malveillante du DNS auraient pris encore plus longtemps. Et je pense que nous voulons conclure cela plus rapidement. Et donc, je dirais que ce n'est probablement pas la façon la plus rapide de procéder. Merci.

JONATHAN ZUCK : Je suis plutôt d'accord, Graeme. Je vois la main levée de Göran. Göran, allez-y. Désolé je ne vous avais pas vu.

GÖRAN MARBY : Merci. En tant que responsable de l'ICANN Org, et j'entends beaucoup de commentaires sur mes chers amis du service de la conformité et de… Je tiens tout d'abord à préciser que la Conformité et l'OCTO travaillent bien entendu ensemble.

Certaines des choses dites sur notre façon de traiter ce que vous appelez les « acteurs malveillants » sont mal informées. Nous croyons fermement que nous essayons de travailler avec les valeurs aberrantes, et nous essayons de changer leur comportement.

Bien que nous nous sommes concentrés sur des acteurs malveillants particuliers, nous l'avons fait. Je ne sais vraiment pas pourquoi cette discussion prend cette tournure. Donc, ce que nous avons dit de…

Tout d'abord, nous pensons, au sein de l'ICANN, que bon nombre de ces discussions appartiennent à la communauté. Nous croyons fermement que les discussions sur l'utilisation malveillante ou son atténuation relèvent de la communauté, tâche dont vous êtes déjà en train de vous acquitter.

Ce qui signifie que, lorsque vous nous demanderez notre avis, la réponse sera bien sûr la suivante : « Nous pensons que cela incombe à la communauté », parce que l'ICANN Org et le Conseil d'administration sont en fait interdits de participer autrement que d'un point de vue factuel aux discussions avec soi-même.

Il y a toujours quelque chose que vous pouvez mettre au point. Il y a toujours des choses que nous pouvons améliorer pour nous et pour le service de la conformité. Mais je le prends un peu… Il y a beaucoup de choses que Jamie a dites ou que l'ICANN Org a dites.

Oui, nous avons des contrats, et je suis d'accord quant au fait qu'un contrat est quelque chose qui se fait entre deux parties. Et nous nous

efforçons, avec les parties contractantes, de comprendre certaines des dispositions qui figurent dans les contrats. Certaines des dispositions, d'ailleurs, ne sont pas issues du processus d'élaboration des politiques, et nous devons nous en occuper.

Donc, je pense que je voudrais juste… La seule question est de savoir si nous avons suffisamment d'outils. C'est-ce que je pense que Jamie essayait de dire… Tout d'abord, nous avons des outils non contraignants et un outil très contraignant.

Le processus qui est mis en place pour ces outils est une chose qui nous impose beaucoup de… Ce n'est pas aussi facile. Nous sommes tenus de le suivre. Et je pense que, en raison du niveau élevé de transparence du processus, il nous faut passer par de nombreuses étapes différentes avant d'obtenir un résultat.

Et puis la discussion aboutit, en quelque sorte, à la conclusion que nous avons déjà des obligations contractuelles, que Jamie n'a pas fait son travail, ou que je n'ai pas fait mon travail, ou que nous n'avons pas les bons outils.

Je pense que ce qui est important dans cette discussion, ce que moi-même [serais venu ici] discuter, c'est comment vous percevez, du point de vue de la communauté, l'utilisation malveillante ? Comment voyez-vous l'utilisation malveillante évoluer ? Que pensez-vous des effets de l'utilisation malveillante qui se sont manifestés avec COVID-19, mais aussi les choses que David a présentées ?

Notre rôle consiste à aider et faciliter cette discussion. Et puis la conformité est, en principe, l'endroit où nous [vérifions] que les politiques figurent dans le contrat et que ce que les politiques ont [établi] depuis le début est effectivement respecté. C'est le rôle du service de la conformité.

Ainsi, pour certains des intervenants qui ont porté ces accusations sur la façon dont fonctionne la Conformité, il semble que vous vous trompez de raisonnement. Vous avez une bonne discussion, je pense, et elle se déroule au bon endroit. Elle appartient à la communauté.

Et dans une certaine mesure, ensuite, elle fait également partie de la discussion sur la mise en œuvre des contrats. Mais, je vous en prie, n'allons pas voir dans ce contexte si le service de la conformité dispose de suffisamment d'outils ou non. Ça doit venir de la communauté.

JONATHAN ZUCK : Merci Göran. Je pense que tout le monde est d'accord. C'est pourquoi nous essayons d'avoir ces conversations. Parce que je pense qu'il y a des gens qui assistent aux réunions, aux appels Zoom, etc., sur ces sujets, et il y en a qui ne le font pas, et je pense que beaucoup des acteurs dont nous parlons dans cette séance particulière sont ceux qui ne le font pas.

Et pourtant, comme l'a dit Graeme, on s'inquiète beaucoup que la réputation de chacun soit dépeinte d'une façon peu soucieuse des

détails. Je pense donc qu'il y a un consensus pour essayer de trouver une solution à ces problèmes, et c'est quelque chose que nous essayons de faire dans la communauté. Brian, avez-vous rapidement quelque chose à ajouter ? Il me semble que nous n'avons plus beaucoup de temps. Cimbolic ?

BRIAN CIMBOLIC : Oui. Merci, Jonathan. Quelques petits points. La disposition du contrat RAA qu'a mentionné Graeme est la section 5.5.2.1.3, qui, pour les opérateurs de DNS existants, serait équivalente à un domaine de cinquième niveau. Elle stipule que l'ICANN peut procéder à une suspension à la suite d'un jugement déclaratoire, lorsqu'un bureau d'enregistrement a permis, par une connaissance réelle ou par une négligence grave,une activité illégale, ou, essentiellement, une utilisation malveillante du DNS. C'est donc un des outils dont dispose l'ICANN auprès des bureaux d'enregistrement.

Je voulais également évoquer le cadre de lutte contre l'utilisation malveillante. Il s'agit d'un accord volontaire. Il est non contractuel. Il comprend des opérateurs de ccTLD, dont certains des plus grands au monde.

On ne voudrait pas dissuader les gens d'y participer, et si on en fait une sorte d'outil de conformité contractuelle, c'est exactement ce qui se produirait.

La seule chose que je dirais aussi, c'est que je vous encourage, si vous trouvez un registre ou un bureau d'enregistrement signataire du cadre de lutte contre l'utilisation malveillante qui ne respecte pas ses obligations, à le dénoncer. Mais il arrive que des gens nous contactent sous les auspices du cadre de lutte contre l'utilisation malveillante, par exemple en cas d'atteinte aux droits d'auteur et en prétendant qu'il s'agit de hameçonnage, alors que ce n'est clairement pas le cas.

Donc, il ne faut pas punir une bonne action. Le cadre de lutte contre l'utilisation malveillante est une bonne chose. Je pense qu'il constitue un pas en avant pour notre secteur, et j'espère que davantage de registres et de bureaux d'enregistrement y souscriront de bonne foi. Mais dans la mesure où vous constatez que ce n'est pas le cas, faites-le savoir.

JONATHAN ZUCK : Merci Brian. Voilà une excellente manière de conclure. Avant de partir, je voudrais juste dire que mes tentatives d'humour noir au début de la séance ont peut-être offensé certains, et si c'est le cas, je m'en excuse. Ce n'était pas mon intention, je voulais juste mettre en commun les gens de tous ces fuseaux horaires.

Je vous remercie donc d'avoir participé à cette conversation. Et je tiens vraiment à remercier David, Graeme et Drew pour leur participation au panel. Je remercie tout le monde de sa participation et de sa contribution à cette séance. Merci. Sur ce, nous clôturons.

[MICHELLE DESMYTER :] Merci beaucoup de nous avoir rejoints.

[FIN DE LA TRANSCRIPTION]