ICANN68 | Forum de politiques virtuel – GAC : atténuation de l'utilisation malveillante du DNS (avec le PSWG) (1/2)
Lundi 22 juin 2020 – 11h30 à 12h30 MYT

GULTEN TEPE : Bonjour. Je demande à l'équipe technique de bien vouloir commencer les enregistrements.

Bonjour, bon après-midi et bonne soirée. Je suis Gulten Tepe de l'équipe de soutien au GAC de l'ICANN. Bienvenue à la séance du GAC de l'ICANN68 sur l'utilisation malveillante du DNS.

Nous n'allons pas faire l'appel aujourd'hui, mais la feuille de présence des membres du GAC sera disponible en annexe du communiqué du GAC ainsi que dans les procès verbaux de cette réunion ICANN68.

Les représentants et délégués du GAC sont encouragés à mettre à jour leur nom ainsi que le pays ou l'organisation qu'ils représentent dans la salle Zoom. Cela nous aidera à tenir les registres de présences et à faciliter la queue pour répondre aux questions pendant la séance.

Si vous souhaitez poser une question ou faire un commentaire, veuillez le taper dans le chat en ajouter au début et à la fin de votre phrase le mot « question » ou « commentaire ». Merci d'être bref.

Le service d'interprétation simultanée sera disponible pour le GAC dans les six langues des Nations Unies ainsi que le portugais à travers à la fois Zoom et la plateforme d'interprétation simultanée à distance

de Congress Rental Network. Des informations sur comment installer et utiliser l'application CRN seront disponibles dans la fenêtre du chat.

Notre équipe de soutien vérifie la salle Zoom et c'est cette équipe, la seule, qui pourra activer ou désactiver les micros. Si vous souhaitez parler, levez la main dans la salle Zoom. Quand vous prendrez la parole, assurez-vous d'avoir mis en silencieux tous vos autres dispositifs.

Et maintenant, je vais donner la parole à Manal Ismail.

PRESIDENTE MANAL ISMAIL : Merci beaucoup Gulten.

Bonjour à tous pour cette deuxième séance du GAC qui va traiter de la question de l'atténuation des risques liés au DNS. Nous aurons deux séances dédiées à ce sujet, une intercommunautaire plus tard et une autre jeudi. Les membres du groupe PSWG vont diriger cette séance qui aura lieu de 3h30 à 4h30 UTC.

Maintenant, je vais passer la parole à Laureen Kapin. Je ne sais pas qui va commencer. Laureen ?

GABRIEL ANDREWS : Bonjour, bon après-midi, bonsoir. Je vois que nous avons plusieurs sujets dont nous allons parler aujourd'hui.

Nous allons parler des leçons tirées à partir de la réponse à la covid-19 de la perspective des parties prenantes de l'ICANN et de la perspective

également des forces de l'ordre et des autorités publiques. Ensuite, nous allons passer en revue les récents développements liés à l'abus du DNS, ensuite les prochaines étapes pour le GAC et les différentes séances de l'ICANN68 concernant l'abus du DNS qui pourraient intéresser les membres du GAC. Diapositive suivante s'il vous plaît.

Au cours des dernières semaines, nous avons pu tirer des leçons très intéressantes par rapport à l'enregistrement de noms de domaine liés à la covid-19. Nous avons tiré des informations de différentes présentations qui ont été faites par le bureau du CTO ainsi que d'autres équipes des forces de l'ordre.

Tout d'abord, les gestionnaires de ccTLD ont indiqué avoir pris des mesures proactives pour vérifier l'identité des titulaire des nom de domaine et pour vérifier les enregistrements avec les forces de l'ordre et les équipes d'intervention informatique d'urgence.

Nous avons pu voir un pic dans les enregistrements liés à la covid-19, dont une partie très faible liée à des activités malveillantes. Vous allez voir également ces informations via les informations qui ont été données par d'autres acteurs.

Il y a également le cadre de mesures à mettre en œuvre par les opérateurs de registre pour répondre à la menace de sécurité qui a été mis en place. Donc en traçant ce cadre, les opérateurs de registre peuvent éviter l'enregistrement de certains noms. Ce cadre constitue un effort important pour pouvoir collaborer avec les forces de l'ordre.

Et la plupart des bureaux d'enregistrement ont agis de manière responsable, et cela mérite d'être reconnu.

Pour ce qui est des parties contractantes, elles ont indiqué une quantité très faible d'enregistrements liés à des activités malveillantes. Et vous allez voir que 70 % des ces enregistrements ont été parkés et non utilisés, contre un petit pourcentage qui ont été utilisés pour des activités illégitimes et 0,5 % ont été liés à des activités malveillantes.

Il y a eu également des indications de signalement par rapport à certaines blacklists qui ont été trop agressives. Donc on a vu des sites qui ont été inclus dans ces listes de façon erronée. Il a été important par la suite de déterminer quelles étaient les activités qui pouvaient avoir un effet malveillant ou pas à partir des observations. Diapositive suivante s'il vous plaît.

L'analyse qui a été menée par le bureau de la technologie de l'ICANN, je l'ai trouvé fascinante. Il y a eu un système qui a été créé pour assurer le signalement d'activités malveillantes. Et cela concernait la création de noms de domaine liés à la covid-19 dans 15 langues différentes, ce qui était assez ambitieux.

Il y a eu également des étapes de validation comparées avec d'autres sources Open Source, par exemple en anglais le mot coordination est lié au mot corona, donc il y a eu un suivi de ce type de noms. On a identifié des milliers d'enregistrements de noms de domaine liés à la pandémie. Et même résultat, il y a eu beaucoup d'enregistrements

mais un nombre très faible de ces enregistrements ont été utilisé pour des activités malveillantes. Ce rapport est très intéressant, je vous invite à le lire, je pense que cela vaut la peine. Diapositive suivante s'il vous plaît.

Maintenant, je vais vous parler d'une autre perspective. Et je voudrais reconnaître qu'il y a plusieurs agences, plusieurs pays dans cet effort qui ont suivi différents processus. Mais je vais vous parler au nom de ma propre agence, le FPI des États-Unis. Donc ce sera centré sur le cas des États-Unis mais je veux reconnaître que nous ne sommes pas les seuls à faire cet exercice.

Les forces de l'ordre vont toujours poursuivre les délinquants. Et nous allons essayer d'identifier ceux qui veulent profiter de la pandémie pour mener des activités malveillantes. Mais bien avant, nous avons pris la décision d'être aussi transparents que possible pour ce qui est des signalements que nous allions recevoir et de partager autant que possible toutes les informations anonymisées que nous allions recevoir. Autrement dit, nous voulions aller chercher le délinquant et non pas seulement attendre à ce qu'il vienne.

Et c'est important du point de vue des parties contractantes aussi parce qu'au lieu de commencer avec des milliers d'enregistrements, nous avons commencé avec un nombre beaucoup plus réduit, avec des centaines, même moins. Et nous allons analyser les signalements que nous avons reçus par rapport à ces domaines comme ayant été la source d'activité malveillante ou source d'hameçonnage.

Ces signalements venaient non seulement du bureau du FBI mais aussi d'autres centres de lutte contre la criminalité. Ces sources incluaient également des données qui venaient du secteur privé, de partenaires comme Microsoft par exemple et qui pouvaient regarder en temps réel tout ce qui se passait sur leurs serveurs et nous en informer par rapport aux noms qui étaient liés à la pandémie pour mener des activités malveillantes. Fishlabs a aussi partagé avec nous des informations très importantes concernant des fraudes.

Tout cela pour vous dire à quel point ce travail a été un effort en partenariat avec différents acteurs, certains partenariats entre les fonctionnaires liés à la sécurité publique et le secteur privé. Je veux insister sur l'importance d'avoir eu ces informations. Nous étions très inquiets par rapport aux faux positifs et nous avons analysé toutes les plaintes. Et au fur et à mesure que nous faisions ces analyses, nous avons reçu de plus en plus d'informations que les bureaux d'enregistrement pouvaient trouver utiles pour pouvoir évaluer les enregistrements. Nous avons compté sur l'aide de RiskIQ pour des captures d'écran, nous avons pu voir quel était le nombre de virus, les codes EPP également pour essayer de minimiser toutes les activités malveillantes. Et dans la mesure du possible, nous avons essayé d'inclure d'autres informations comme les outils de domaines API. À partir de ces signalements, nous avons contacté les registres concernés pour préserver ces informations.

Je vais aborder un point qui est un peu plus difficile maintenant. Diapositive suivante s'il vous plaît. Vous voyez ici les chiffres. Nous

avons reçu 1 349 signalements de domaines au 6 décembre 2020. Ce chiffre aurait pu être beaucoup plus élevé mais nous voulions éviter les faux positifs et nous avons seulement accepté les domaines sur lesquels les bureaux d'enregistrement pouvaient agir. S'il vous plaît, pouvons-nous passer à la diapositive ? Très bien.

Nous avons reçu ces informations de manière hebdomadaire. Et le pic a été enregistré le 17 avril avec plus de 350 signalements. Diapositive suivante.

Cette diapositive, nous l'avons piquée de la présentation de l'OCTO et vous voyez ici que le pic d'enregistrements de noms de domaine liés à la covid-19 a eu lieu autour du 5 mai alors que le nôtre était le 17 avril. Donc la courbe apparaît comme suivant le même schéma que celui de l'OCTO mais avec un décalage de quelques semaines. On a donc cette différence de temps entre le moment de l'enregistrement et l'utilisation de ces noms de domaine. Cela montre que les signalements des forces de l'ordre qui sont valables parce qu'ils rapportent ce que l'on voit dans le monde réel ne vont pas toujours être réactifs. Et rarement, ces signalements vont être proactifs. En général, ils interviennent après les faits. Donc les efforts proactifs sont dans les mains des bureaux d'enregistrement eux-mêmes.

Pour ce qui est du nombre de bureaux d'enregistrement par rapport auxquels nous avons reçu des signalements, 104. Ici, vous voyez les 10 plus importants avec un pic sur la droite. GoDaddy faisait partie de ces bureaux d'enregistrement qui étaient très communicatifs et qui ont été très réactifs. Il y en a d'autres qui sont sur la liste des 10 principaux

qui ont aussi été très réactifs mais qui n'avaient pas forcément la même part de marché.

Il y a eu des instances d'hameçonnage, bien entendu, mais d'autres types de fraudes et je vais vous donner un exemple. Dans notre bureau de Boston, on a identifié une famille qui recevait des menaces à la maison. Il paraît que quelqu'un vendait des masques pour la covid-19 chez eux, donc la personne mettait leur adresse. Ceux qui payaient pour les masques et ne les recevaient jamais, c'était l'adresse qu'ils avaient où réclamer, donc ils réclamaient à cette famille.

Le bureau d'enregistrement a pris le nom de la famille qui a été utilisé sans permission, il a pu répondre. Et vu la menace physique, ils ont dû prendre des mesures. C'est le type de réponse que nous apprécions, nous, les collègues Boston, et sans doute la famille qui faisait l'objet de la menace. Et c'était un des 1 300 signalements.

C'est sûr que les différents bureaux d'enregistrement doivent recevoir suffisamment d'informations pour prendre des mesures pour protéger les personnes qui font l'objet de menaces en raison de l'utilisation malveillante de leurs données.

Maintenant que je leur ai fait doré un peu la pilule, je vais parler de leurs faiblesses. Souvenez-vous que j'avais dit qu'il fallait envoyer des lettre de conservation pour les domaines signalés et voilà pourquoi : 65 % des domaines que nous avons identifiés montraient qu'ils avaient utilisé un service d'enregistrement fiduciaire ou de confidentialité, anonymisation. Or, je vous rappelle que le

fonctionnaire de sécurité publique qui enquête sur ce cas de fraude ou d'hameçonnage identifie plein de cas par semaine. Or, ce qu'il faut faire immédiatement pour se mettre au travail sur les délinquants les plus prolifiques qui font cela, il faut identifier tout de suite ou aussi vite que possible de qu'il s'agit, donc il faut hiérarchiser ces efforts, les classer par ordre de priorité. Or, nous avons décidé que nous ne pouvions pas le faire en temps réel ; ce n'était simplement pas faisable.

Suivant la politique de l'ICANN et tel que cela fait partie de nos politiques à l'heure actuelle, les services d'enregistrement fiduciaire et d'anonymisation doivent répondre aux demandes de sécurité publique pour les enregistrements. Et par la suite, les informations sont envoyées pour des procès juridiques, c'est-à-dire pour des tribunaux ou de citations judiciaires. En général, cela prend 30 secondes pour chercher les données WHOIS s'il n'y a pas eu de service d'anonymisation ou d'enregistrement fiduciaire qui était engagé. Or, avec l'utilisation de ce type de service, cela prend en moyenne trois semaines pour obtenir ces mêmes données.

Par conséquent, pour nous assurer que ces données seront disponibles pour répondre aux procès juridiques, on envoie des lettres pour faire le suivi de ces procès juridiques, des lettres de conservation. Cela implique plus de travail pour nous, plus de travail pour les bureaux d'enregistrement mais cela pourrait être la nouvelle norme. Diapositive suivante.

Quant aux délits généraux sur internet, dans le cadre de cette pandémie de la covid-19, il est à remarquer que pendant que nous sommes pendant plus longtemps chez nous devant l'ordinateur à travailler devant l'écran, on voit plus de cas de criminalité et d'utilisation malveillante. En avril 2020, on a reçu plus de deux fois et demie la quantité de plaintes qu'on avait eues en avril 2019. On est donc dans une période vulnérable et c'est pourquoi il faut être plus surveillants, plus attentifs. Il me semblait qu'il était important de signaler cela.

Voici la dernière diapositive sur la question de la covid-19. Je voudrais signaler que ma collègue Laureen représentera le GAC dans la séance plénière intercommunautaire de l'ICANN68 qui suivra immédiatement cette séance. Parlant de Laureen, je vais demander à ce que l'on active son micro pour lui céder la parole pour qu'elle présente elle-même les diapositives suivantes.

LAUREEN KAPIN : Merci. Je pense que vous m'entendrez maintenant ; c'est ce que j'espère en tout cas. Mon micro s'affiche allumé. Donc je vais vous demander de passer à la diapositive suivante.

Je vous remercie tous de participer à cette séance. Je sais que ce n'est pas une heure très accommodante pour certains parmi vous, donc je vous en remercie.

Je vais me concentrer sur certains développements récents au sujet de l'utilisation malveillante du DNS. Certains développements ont été bien accueillis, d'autres posent des défis.

Très récemment, il y a quelques jours, les bureaux d'enregistrement et les opérateurs de registre qui sont des parties contractantes ont adopté une définition de l'utilisation malveillante du DNS. Ces parties contractantes ont indiqué que la définition était composée de cinq catégories générales d'activités nuisibles du fait qu'elles sont superposées avec le DNS. Donc on a le cas du SPAM qui comprend un lien qui pourrait installer du logiciel malveillant sur votre ordinateur si vous le cliquer. Cela présente un cadre pour pouvoir lutter contre l'utilisation malveillante du DNS mais également pour que l'équipe de révision du choix du consommateur et de la concurrence vérifie que ce soit en conformité avec la définition de l'utilisation malveillante de la sécurité du DNS, des cas d'abus à la sécurité.

Le GAC avait également défini les menaces à la sécurité au préalable et cette définition était cohérente avec la nouvelle définition qu'ont adoptée les parties contractantes. Donc il est important de voir qu'il y a une définition qui ait été accordée par rapport à l'utilisation malveillante du DNS. C'est pourquoi je dis qu'il s'agit d'un développement qui est bien reçu parce qu'il y a un ensemble d'activités malveillantes qui constitue l'utilisation malveillante du DNS en termes généraux mais qu'il faut savoir quelles sont ces activités. On pourrait discuter de l'élargissement de cette liste d'activités qui y sont comprises, mais c'est une toute autre discussion.

Un autre développement lié à cette définition est la recommandation de l'équipe de révision de confiance des consommateurs, recommandation 14, qui discute des initiatives communautaires pour rédiger une définition de l'utilisation malveillante afin d'informer les actions à prendre. C'est une partie très pertinente de la communauté et encore une fois, nous les remercions de cet effort.

Du côté un peu plus difficile de ce bilan, il reste des défis à l'application pour le service de conformité de l'ICANN et ce, en partie en raison de la rédaction des contrats qui définissent les règles applicables pour les opérateurs de registre et les bureaux d'enregistrement. Nous en discuterons davantage, surtout lors de la séance de l'ICANN consacrée aux engagement d'intérêt public et aux défis y afférents. Ce sera également à venir dans quelques heures.

Mais pour vous donner un aperçu un peu général, dans les contrats, il y a des exigences pour que les opérateurs de registre qui ont des exigences en aval fassent respecter les mesures contre l'utilisation malveillante du DNS. Et par cela, j'entends que les contrats disent que les bureaux d'enregistrement doivent avoir des dispositions contractuelles qui existent, l'interdiction à ce que leurs titulaires de nom de domaine utilisent ces enregistrements à des fins malveillantes et que les opérateurs de registre eux-mêmes doivent également surveiller l'utilisation malveillante du DNS.

Or, dans ces contrats, il n'y a pas de conséquences qui soient prévues vis-à-vis de ce problème. Et je dis conséquences s'il y avait quelque chose de mauvais qui arrive. Par exemple, s'il y a une obligation de

surveiller l'utilisation malveillante du DNS de la part des opérateurs de registre, on ne sait pas qu'est-ce qui suit. Une fois qu'on identifie une utilisation malveillante du DNS, il est important de savoir qu'est-ce qui est à suivre. De même, les bureaux d'enregistrement ont l'obligation d'interdire à leurs titulaires de nom de domaine d'utiliser leur enregistrement pour ce type d'abus. Mais il n'y a rien de spécifique qui soit dit par rapport à la réponse qu'ils doivent donner si les titulaires utilisaient leur enregistrement à ces fins malveillantes. Donc il reste des problèmes et des améliorations qui pourraient être apportées à la rédaction des contrats.

Je tiens également à signaler que pour ce qui est de la définition de l'utilisation malveillante du DNS, souvenez-vous que j'ai dit qu'il y avait maintenant un accord fondamental sur ce qu'est fondamentalement l'utilisation malveillante du DNS et spécifiquement sur quelles sont les activités malveillantes qui constituent des menaces à la sécurité du DNS.

Je signale également que l'équipe de révision de la confiance des consommateurs a défini en termes plus généraux la conduite qui pourrait amener à une exploitation malveillante du DNS. Et ce que l'équipe a recommandé – et je le dis très franchement, j'étais présente à leurs débats et j'ai suivi leurs échanges –, ils ont adopté une définition un peu plus large disant qu'il s'agit d'une activités qui est intentionnellement difficile à suivre ou qui est confuse, qui génère des activités non demandées, qui utilise activement le DNS et/ou les procédures utilisées pour enregistrer des noms de domaine. Et cela

n'inclut pas certaines formes d'utilisation malveillante des contenus des sites web. Cela fait allusion au cadre qui s'occupe de l'utilisation malveillante qui prévoyait des exceptions, parce que l'abus des contenus est tellement difficile à gérer qu'il faut avoir à chaque fois des dispositions spécifiques. Mais l'équipe de révision qui s'est centrée sur ces questions recommande que l'on adopte une définition plus large de l'utilisation malveillante du DNS afin de comprendre les différentes activités qui sont nuisibles pour le DNS.

On a vu des progrès accomplis pour pouvoir adopter une définition par rapport à l'utilisation malveillante du DNS, mais il manque toutefois davantage de discussions pour pouvoir définir un peu mieux ce concept. Diapositive suivante.

Je vois qu'il y a des questions sur le chat. Je conseillerai à ce qu'on revienne sur la présentation à la fin de la séance pour pouvoir répondre à vos questions si on a le temps. Entre Gabe et moi, on essayera de le faire. Je vois que vous avez des questions, c'est pour cela que je dis cela, parce que je veux vous rassurer : on aura du temps pour vos questions à la fin de la présentation.

Il y a d'autres développements liés à l'utilisation malveillante du DNS et j'aborderai à ce point-là des autres recommandations formulées par l'équipe de révision de la confiance des consommateurs. Certaines font l'objet de l'examen du Conseil d'Administration, certaines ont été adoptées, d'autres rejetées et d'autres sont en état d'attente.

L'équipe de révision de la CCT a formulé des recommandations qui ont été cédées ou déléguées au groupe de travail consacré au PDP relatif aux procédures pour les séries ultérieures de nouveaux gTLD qui parlaient de l'atténuation de l'utilisation malveillante du DNS. Mais malheureusement, en avril, il n'y avait toujours pas de plan pour formuler des recommandations sur ce sujet. Il me semble que ce qui nous inquiète est que nous avons des contrats qui s'appliquent aux nouveaux gTLD, des contrats qui portent sur les gTLD historiques, et il y a la possibilité désormais d'avoir une deuxième série et il nous faut des normes. Donc si nous souhaitons améliorer l'écosystème de l'utilisation malveillante du DNS, on pourrait suivre le modèle d'avoir une moyenne plus élevée de sorte que tous les autres doivent suivre et que ce soit l'opportunité de s'améliorer plutôt que de voir cela comme un développement qui soit négatif. En tout cas, il est possible d'avoir d'autres discussions à ce sujet.

Par rapport à cette question des recommandations de l'équipe CCT, voilà ce qu'ils ont dit par rapport à l'utilisation malveillante du DNS. Dans le communiqué de Montréal, le GAC a prononcé un avis selon lequel avant de procéder à une nouvelle série de nouveaux gTLD, les recommandations de l'équipe CCT soient établies comme des prérequis avant de lancer une nouvelle série ou qu'elles soient considérées comme une priorité.

Pour ce qui est du PDP concernant les séries ultérieures, le GAC a exprimé sa préoccupation par rapport à l'approche suivie concernant les nouvelles séries en ce sens qu'il faudrait mettre en œuvre les

recommandations concernant l'utilisation malveillante du DNS avant le lancement d'une nouvelle série.

Actuellement, il y a des consultations en cours par rapport à cette question. Je pense que les problèmes liés à la pandémie de la covid-19 ont servi à pouvoir mieux voir quels sont les risques dans des circonstances exceptionnelles comme des catastrophes naturelles. Nous savons que cela peut inspirer non seulement les gens bienveillants mais aussi les gens malveillants à se réunir. Et pour ces gens qui souhaitent mener des activités malveillantes, ils mettent à profit la pandémie ou la catastrophe naturelle pour mettre en œuvre leurs actions délictuelles. Diapositive suivante s'il vous plaît.

Je voulais faire référence également aux activités d'un autre groupe important et la révision SSR2, la révision de la sécurité, la stabilité et la résilience. Il y a dans cette révision des recommandations qui visent l'atténuation des risques liés à l'utilisation malveillante du DNS. Le GAC a participé à la consultation publique en renforçant l'importance de ces recommandations. Un point important sur lequel nous avons insisté, ce sont les efforts pour renforcer le système DAAR, le système de signalement des cas d'utilisation malveillante des noms de domaine. Et nous attendons les recommandations finales de cette équipe en octobre.

Un autre développement important que nous saluons, c'est le travail du SSAC. Un groupe de travail a été créé au sein du SSAC qui s'occupe de la question de l'utilisation malveillante du DNS. Nous avons un groupe d'experts importants qui travaillent là-dessus et nous saluons

leur travail. Il y a un certain nombre de sources qui peuvent être intéressantes, comme les blacklists, etc. Ils se focalisent également sur les approches innovatrices qui apparaissent dans le secteur et dans l'industrie, les approches pour les ccTLD ainsi que de nouvelles approches ou des recommandations qu'ils peuvent élaborer pour la communauté de l'ICANN.

Un membre de l'équipe de travail sur la sécurité publique est invité à faire partie de ce groupe du SSAC. Le SSAC aura une séance publique mardi 23 juin 2020 à 12h30 UTC si vous êtes intéressé à y participer.

Je voulais montrer aux collègues du GAC ou aux personnes présentes à cette réunion qu'il y aura un certain nombre de séances de l'ICANN68 consacrées à la question de l'abus du DNS. Il y aura une séance de préparation pour la réunion avec le Conseil d'Administration qui aura lieu à 7h00 UTC ce lundi. Il y aura une deuxième séance plénière du GAC sur l'abus du DNS mardi et ensuite, il y aura une réunion avec le Conseil d'Administration mercredi.

Parmi les sujets que nous prévoyons aborder dans ces séances figure la question des services d'anonymisation et d'enregistrements fiduciaires. Gabriel a évoqué très brièvement cela. Ce type de services peuvent rendre les efforts plus difficiles parce qu'il est difficile de savoir qui est derrière une activité malveillante. Il y aura également une discussion par rapport aux mesures proactives anti-abus et cela, en lien avec les recommandations de l'équipe de révision CCT et ensuite, finalement, le système de signalement portant sur l'exactitude du WHOIS.

Le GAC a participé à ces évaluations de l'exactitude des informations d'enregistrement. À un moment donné, les activités ont été suspendues pour analyser la spécification temporaire et tous les changements liés à la mise en œuvre du RGPD. Il y a eu une recommandation pour que ce projet commence à nouveau ou reprenne ses activités pour pouvoir évaluer l'exactitude de l'identité liée à un enregistrement. Donc cela ajoute une troisième étape concernant l'exactitude des données. Donc on lance un appel pour que ce projet puisse se remettre en marche. Diapositive suivante s'il vous plaît.

Maintenant, je sais que ces informations ont été distribuées sur la liste de diffusion du GAC, mais je vais évoquer certaines questions que l'on pourrait poser au Conseil d'Administration de l'ICANN. Gabriel, je pense que vous allez passer en revue la première question sur le service d'anonymisation et d'enregistrement fiduciaire.

GABRIEL ANDREWS : Je vais parler un petit peu de la notion des services d'anonymisation et d'enregistrement fiduciaire parce que je voudrais rappeler pourquoi cette question existe.

Nous avons dit que pendant cette pandémie, les forces de l'ordre ont reçu un nombre très important de signalements d'activités malveillantes, mais qu'il y avait la possibilité qu'il y ait des faux positifs. Mais la plupart de ces signalements se trouvaient derrière des services d'anonymisation et d'enregistrement fiduciaire. Donc la

question est de savoir : que doit-on faire pour savoir si ces services d'anonymisation et d'enregistrement fiduciaire doivent continuer ou non à la lumière de la révision CCT pour pouvoir, nous, protéger les utilisateurs et identifier ceux qui se cachent derrière ce service ?

LAUREEN KAPIN : Merci Gabriel. Le petit silence est dû au fait que cela prend un certain temps pour le micro de s'allumer.

Nous allons parler également de mesures anti-abus proactives. L'équipe de révision CCT a recommandé que l'ICANN négocie des dispositions contractuelles afin de mettre en place des encouragements pour les parties prenantes qui adopteraient des mesures anti-abus proactives. Cette recommandation vise à encourager ces mesures proactives. Cette recommandation se trouve encore en suspens.

Pour ce qui est des questions, on voudrait savoir s'il y aura des efforts de facilités pour développer une définition d'abus. Et nous aimerions savoir quels sont ces efforts au niveau de la communauté.

Nous avons également une question : pourquoi les définitions existantes par rapport à l'abus du DNS ne sont pas suffisantes ? Et la dernière question : est-ce que l'ICANN considère la possibilité d'encourager la validation des informations des titulaires de noms par les bureaux d'enregistrement et cela, pour s'assurer que les informations que vous recevez concernant les titulaires de noms – leurs noms, leurs autres informations – sont exactes car il y a des

registres et des bureaux d'enregistrement qui réalisent ce type de validation ? Diapositive suivante s'il vous plaît.

La question suivante concerne l'exactitude des données d'enregistrement gTLD. Cette question est liée à cette dernière question que je viens d'évoquer. Le manque d'exactitude constitue un problème par rapport aux informations d'enregistrements de noms de domaine et ce problème a été signalé depuis longtemps. Vous avez sur l'écran des informations de contexte. La première équipe de révision du WHOIS a signalé certains problèmes au niveau de l'exactitude des informations WHOIS. L'équipe de révision CCT a recommandé de reprendre le travail de ce projet pour mettre en place une dernière étape de validation d'identité. Cette recommandation est encore en suspens. Maintenant, nous avons l'équipe de révision CCT2 qui recommande la même chose, et cette recommandation est aussi en suspens en attendant que l'équipe d'élaboration de la spécification temporaire finisse son travail.

Maintenant, nous savons que l'étape 2 de l'équipe EPDP n'aura pas de recommandations liées à l'exactitude de ces informations. Il n'y a pas trop de perspectives pour reprendre le travail de ce projet. Sachant que le problème de l'exactitude reste une inquiétude permanente, la question est de savoir ce que le Conseil d'Administration entend faire pour essayer de répondre à ce problème de l'inexactitude des informations d'enregistrement, y compris la possibilité de remettre en route ce projet qui a été mis en suspens. Diapositive suivante s'il vous plaît.

Je pense qu'on arrive à la fin de la présentation. Vous voyez ici, nos annonces d'autres séances de l'ICANN68 que vous pourrez trouver intéressantes par rapport à cette question. Si vous le souhaitez, vous pouvez participer à ces autres séances plénières de l'ICANN. Il y aura la séance plénière sur l'abus du DNS et les enregistrements malveillants pendant la pandémie de la covid-19 plus tard aujourd'hui. Il y aura une séance sur le DNS et l'internet des objets, opportunités, risques et difficultés. Nous savons que depuis Alexa jusqu'au chauffage de la maison, les voitures, l'internet des objets fait partie de notre vie quotidienne. Et en plus de nous faciliter la vie, cet internet des objets présente aussi des difficultés ou des risques. Ensuite, il y aura des séances d'At-Large qui vont traiter de cette question. Il y aura une séance dédiée à l'abus du DNS, covid-19 et problèmes des utilisateurs finaux ce lundi plus tard. Ensuite, abus du DNS, établir un seuil acceptable. Et finalement, nous avons une séance de la ccNSO qui va s'occuper des ccTLD et la pandémie de la covid-19. Comme vous le voyez, c'est un sujet brûlant qui sera abordé dans plusieurs des séances depuis différentes perspectives.

Ceci dit, je pense que nous sommes arrivés à la fin de notre séance. Et nous aurons l'occasion de répondre à des questions. Je vais céder la parole à Manal qui lève la main. Il me semble que c'est bien la meilleure manière de pouvoir commencer avec cette séance de questions et réponses. Manal, allez-y.

PRESIDENTE MANAL ISMAIL : Merci Laureen et Gabriel pour cette présentation qui était fort intéressante. Je vais essayer de suivre les questions. J'espère ne pas en avoir omis.

La première question venait du représentant du Népal et disait : « Est-il possible d'expliquer l'utilisation malveillante du DNS compte tenu des logiciels malveillants, des réseaux zombie, du hameçonnage, du phishing et du SPAM à l'aide d'un schéma ou d'un algorithme plutôt que d'avoir des phrases générales pour qu'il soit plus facile de comprendre de quoi il s'agit ? »

LAUREEN KAPIN : Je cèderai maintenant la parole à Gabriel pour qu'il réponde.

GABRIEL ANDREWS : Merci.

En peu de mots, l'idée est de ne pas céder le pouvoir de définir cela aux forces de police. Mais il y a des schémas graphiques qui peuvent être utilisés. Peut-être que je le ferai dans d'autres présentations, je n'en ai pas maintenant. Mais je pense que surtout s'agissant des réseaux zombie, ce sont des choses qui sont plus faciles à voir lorsqu'on a une image, de manière visuelle. Donc oui, je prends note de votre commentaire pour nos discussions à l'avenir.

PRESIDENTE MANAL ISMAIL : Merci Gabriel.

Il y avait une autre question de [Soulane] qui disait : « Avons-nous reçu des réponses concernant la lettre de l'équipe de travail SubPro sur la décision de ne pas prendre des mesures vis-à-vis de l'utilisation malveillante du DNS ? Cette décision n'est-elle pas considérée dangereuse à la lumière des chiffres en augmentation que vous avez présentés ? »

J'espère que Keith ne sera pas gêné mais je vais lire la réponse qu'il a fourni sur le chat où il disait : « Le groupe de travail du PDP à envoyé une lettre au conseil de la GNSO et il y aura une discussion sur les prochaines étapes possibles vis-à-vis de ces recommandations liées au CCTRT, donc il aurait différents choix à faire qui seraient informés par cet objectif de déterminer la meilleure voie pour lutter contre l'abus. »

J'ai également un commentaire de Becky Burr qui demandait : « Laureen, vous avez évoqué la portée élargie de l'utilisation malveillante du DNS évoquée dans la révision de la CCT. Vous avez indiqué que le contenu n'est pas dans la portée de cette définition. Pouvez-vous nous aider à comprendre où en est la limite ? Par exemple, certains exemples de l'utilisation malveillante du DNS qui correspondent à la mission de l'ICANN ne correspondent pas aux comportements identifiés par la CPH (des comportements qui sont identifiés comme des abus à la sécurité par l'équipe CCT). »

Laureen, est-ce que je peux vous céder la parole ?

LAUREEN KAPIN : Oui, tout à fait. C'est une bonne question, elle est très juste.

J'aimerais avoir le rapport sous les yeux parce que je suis sûre qu'il doit contenir des exemples de cela. Mais Becky, je pense qu'il serait mieux de pouvoir chercher ces informations spécifiquement pour pouvoir voir ce qu'on en a dit l'équipe. J'imagine que cela a trait à l'étude sur le DNS qui était demandée par l'équipe de révision de la CCT qui a partagé des statistiques d'intérêt liées à certains exemples d'abus systémiques du DNS. Je crois que s'il y avait des cas d'activités malveillantes spécifiques ou des informations trompeuses qui étaient transmises à travers l'utilisation d'un nom de domaine, cela pourrait ne pas être dans la portée du travail de sécurité du DNS, que cela pouvait ne pas faire partie de l'utilisation malveillante du DNS comme tel mais que cela pouvait constituer une exploitation du DNS et par conséquent, être toujours dans la portée de la mission de l'ICANN parce qu'il s'agirait d'une exploitation du DNS. Mais je voudrais être sûre de cela et le vérifier.

En tout cas, cela pourrait être un exemple qui aide à considérer la question. Et dans le contexte de la covid-19 par exemple, c'est exactement le type de scénario dans lequel les forces de l'ordre ont échangé avec les bureaux d'enregistrement pour évaluer le cas des noms de domaine en particulier parce qu'il s'agit de noms de domaine qui ont spécifiquement un sens ou un message intrinsèque de tromperie. Par exemple si on a un nom de domaine qui dit cure pour la covid-19 ou vaccin covid-19, il n'existe pas de vaccin qui soit efficace en tout cas, on n'a pas de cure qui soit efficace, donc le message de ce

nom de domaine pourrait être problématique. Il pourrait y en avoir d'autre mais j'espère que cet exemple aura été utile pour répondre à votre question.

PRESIDENTE MANAL ISMAIL : Merci beaucoup Laureen.

J'espère ne pas avoir oublié d'autres questions qui aient été posées sur le chat. Il y avait des discussions intéressantes sur le chat et je voudrais inviter tout le monde à suivre les débats qui y ont eu lieu. Si j'ai oublié de lire un commentaire ou une question que vous avez posée sur le chat, partagez-la à nouveau pour que je puisse la lire à haute voix.

Y a-t-il d'autres questions ou commentaires ? Je n'en vois plus d'autres.

Merci Laureen et Gabriel pour cette présentation intéressante.

Vous allez récupérer cinq minutes. On aura maintenant une pause de 30 minutes. Assurez-vous de participer à la plénière intercommunautaire sur l'utilisation malveillante du DNS et les enregistrements malveillants dans le cadre de la covid-19 qui est prévue pour 1h30, de 13h00 à 14h30 heure de Kuala Lumpur ou autrement 5h00 à 6h30 UTC. Laureen participera et l'équipe du PSWG était parmi les organisateurs de la séance. Ce panel sera suivi d'une pause de 30 minutes et nous allons nous réunir à nouveau dans la salle du GAC après cela. Donc soyez de retour dans la salle à 15h00

heure de Kuala Lumpur, 7h00 UTC, pour nous préparer à notre réunion avec le Conseil d'Administration.

Merci à tous et profitez de la pause.

[FIN DE LA TRANSCRIPTION]