ICANN69 | Réunion générale annuelle virtuelle – Utilisation malveillante du DNS
Mardi 20 octobre 2020 – 10h30 à 12h00 CEST

OZAN SAHIN : La séance va commencer. L'enregistrement commence.

Bonjour, bienvenue à la séance plénière sur l'utilisation malveillante du DNS. Je m'appelle Ozan Sahin. Je vais m'occuper de l'administration de cet appel à distance.

Veuillez noter que cette séance est enregistrée et respecte le code de conduite attendu de l'ICANN.

Pendant cette séance, les questions ou commentaires ne seront lus à haute voix que s'ils sont soumis en anglais dans l'onglet Q&A, donc questions et réponses. Vous y avez accès dans la barre de Zoom. Je vais lire les questions et commentaires à haute voix lorsque le modérateur de la séance me l'indiquera.

Cette séance inclut l'interprétation et la transcription en temps réel. Pour y avoir accès, cliquez sur *closed caption* dans la barre d'outils en bas. L'interprétation pour cette séance se fera en arabe, en chinois, en anglais, en français, en russe et en espagnol. Vous y accéderez en accédant à la plateforme d'interprétation simultanée à distance opérée par Congress Rental Network. Les participants sont encouragés à télécharger l'application de la plateforme en suivant les

indications sur le chat de Zoom ou sur les documents disponibles sur le site web de la conférence.

Si vous voulez intervenir, levez la main dans la salle Zoom et une fois que le modérateur de la séance vous appelle, nos techniciens vous permettront d'activer votre micro. Veuillez alors indiquer votre nom pour la transcription et la langue dans laquelle vous allez intervenir si vous allez intervenir dans une autre langue que l'anglais.

Une fois que vous interviendrez, assurez-vous de mettre sur muet tous vos autres dispositifs et applications, dont la plateforme d'interprétation simultanée à distance. Veuillez parler distinctement et à un rythme raisonnable pour permettre une interprétation précise.

Et j'aimerais vous indiquer que les participants à distance ne peuvent pas cliquer sur l'icône micro et activer leur micro, ce sont nos techniciens qui vont le faire. Vous pouvez faire des commentaires sur le chat. Pour ce faire, utilisez le menu déroulant sur l'icône chat et ainsi, tout le monde pourra voir vos commentaires. Veuillez noter que les chats privés ne sont possibles qu'entre les membres du panel sur ce format de webinaire Zoom. Ces commentaires seront également vus par les présentateurs.

Sur ce, je vais céder la parole maintenant à Thomas Rickert. Thomas, c'est à vous.

THOMAS RICKERT : Merci beaucoup Ozan.

Bonjour, bon après-midi, bonsoir à tous. Je m'appelle Thomas Rickert. Je travaille avec l'industrie qui est d'ailleurs co-organisateur de l'ICANN69. Je suis dans mon pays d'origine, l'Allemagne. J'aurais souhaité vous recevoir cette fois-ci mais ce n'est que partie remise. J'espère que nous aurons l'occasion de nous revoir très prochainement et j'espère que vous vous portez bien. Passons à la diapositive suivante s'il vous plaît.

Comme Ozan vient de le dire, cette séance porte sur l'utilisation malveillante du DNS. Et il y a eu beaucoup d'attention portée à cette question. Je pense que la raison pour laquelle cette question nous occupe énormément, c'est parce qu'il y a beaucoup de mauvaises choses qui ont lieu sur l'internet et que beaucoup de mauvais acteurs sont en train d'essayer d'exploiter à mauvais escient l'absence de connaissances des utilisateurs et essaient de les fourvoyer en engendrant des dommages financiers, entre autres. Donc je pense que pour l'ICANN, c'est une thématique très spéciale étant donné le mandat très limité de l'ICANN conformément à ses statuts constitutifs, d'où l'importance de poursuivre ce dialogue sur l'utilisation malveillante du DNS, bien comprendre ce qui est en jeu, quel est le problème, quels sont les rôles et responsabilités des différentes parties prenantes et acteurs de l'écosystème de l'internet et voir aussi quelles sont les solutions ou pas vers l'avant potentiels. Je pense qu'on va essayer aujourd'hui de se concentrer sur les solutions et sur les pas en avant à effectuer.

Aujourd'hui, on a une séance de 90 minutes, et comment allons-nous organiser cette séance ? Nous allons avoir des présentations de la part

des intervenants que je vais vous présenter dans un instant. Et ensuite, nous allons faire une pause après chacune de ces interventions, très brièvement, pour voir si vous avez écrit des questions sur l'onglet Q&A. Nous allons essayer de répondre aux questions à mesure qu'elles sont postées sur l'onglet et veuillez indiquer les questions qui sont liées à l'intervenant. Si vous avez des doutes par rapport à la présentation qui vient d'être faite, n'hésitez pas à nous en faire part. Mais sachez que de toute façon, à la fin de toutes ces présentations, nous allons avoir une séance de questions et réponses. Vous aurez donc l'opportunité de poser des questions d'ordre général et vous pouvez le faire sur l'onglet Q&A mais aussi en levant la main, et nos techniciens vont ensuite activer votre micro pour vous permettre d'intervenir. Donc vous pourrez également intervenir oralement. Voilà pour ce qui est des remarques liminaires puisqu'on va maintenant passer au vif du sujet dans un instant.

Je vais vous présenter un petit peu nos intervenants aujourd'hui. Aujourd'hui, nous avons avec nous David Conrad, Jeff Bedser, Mason Cole, Chris Lewis-Evans, James Bladel. Puis nous allons avoir une discussion tous ensemble. Et pendant les dernières minutes, je vais essayer de faire un petit résumé et récapituler un petit peu tout ce que l'on aura entendu. Passons à la diapositive suivante s'il vous plaît. C'est déjà la première diapositive de David, je me suis trompé. Voilà un petit peu l'organisation de la séance aujourd'hui. Et sans plus attendre, je vais céder la parole à David Conrad, du bureau du directeur de la technologie OCTO, qui va nous parler de l'utilisation malveillante du DNS.

DAVID CONRAD : Merci beaucoup Thomas.

En vue de cette plénière, on m'a demandé de préparer une présentation pour essayer de refléter un petit peu le paysage des menaces à la sécurité des domaines entre septembre 2019 et septembre 2020. Si vous regardez les rapports DAAR, signalements des cas d'utilisation malveillante disponibles sur le site web de l'ICANN, vous verrez que les données publiées dans ces rapports remontent à 9 mois. Excusez-moi, il y a une faute de frappe ici sur la diapositive, qui indique six mois.

Mon équipe a élaboré des statistiques générales et au cours de la dernière année, vous voyez une décroissance dans les logiciels malveillants. Et en raison de la prévalence des spam, dans ces statistiques d'utilisation malveillante du DNS, vous voyez un petit peu la situation.

La conclusion générale de l'année entre 2019 et 2020, c'est que le nombre d'utilisations malveillantes de domaines a augmenté d'environ 13 %, mais le ratio général d'utilisation malveillante en raison des décroissances et autres s'est plus ou moins maintenu.

Les données toutefois qu'on a au sein de DAAR remontent à octobre 2017. Et si vous regardez un petit peu plus en arrière, vous verrez qu'il y a certaines tendances relativement claires qui nous montrent que le nombre de gTLD bien entendu augmentent. Et vous voyez ici

différentes augmentations au fil du temps, mais la tendance est assez claire.

Sur le deuxième graphique, vous voyez ici le nombre de menaces à la sécurité agrégé qu'on a examiné dans le cadre du rapport DAAR par rapport à la distribution des logiciels malveillants et des courriels indésirables. Vous voyez ici la tendance au fil du temps qui va en décroissance ; c'est assez clair aussi.

Si vous regardez maintenant le graphique numéro 3, vous voyez ici une normalisation en fonction du nombre de domaines dans une zone particulière. Là encore, ce que vous voyez, c'est une tendance à la baisse au fil du temps, avec une légère croissance sur la fin.

Ensuite, sur le graphique 4, vous voyez qu'en rouge, ce sont les spams, donc les courriels indésirables. Et les autres points à noter sur ces quatre graphiques, c'est que cette ligne, qu'elle soit rouge ou bleue, vous indique l'entrée en vigueur du RGPD. Et vous noterez que sur ces graphiques, il n'y a pas eu d'impacts significatifs sur le nombre d'utilisation malveillante du DNS, en tout cas détectables dans le cadre du contexte du DAAR, rapports sur les cas d'utilisation malveillante du DNS.

Si vous voyez maintenant les menaces individuelles pour cette même période, de octobre 2017 à septembre 2020, là encore, vous voyez que dans ces délais, il y a des effets intéressants. Cela, on le compare aux statistiques que je vous ai montrées dans la diapositive précédente où le hameçonnage, les logiciels malveillants, etc. étaient en baisse. Mais si vous regardez ce qui se passait en octobre 2017, vous voyez que

c'est l'inverse puisque le hameçonnage, les logiciels malveillants et les *command and control* de réseaux zombie augmentaient alors que les courriels indésirables étaient à la baisse.

Et il faut être prudent par rapport à ces graphiques parce qu'il faut s'assurer de comparer les bons éléments de manière verticale et horizontale et il faut bien prendre soin d'analyser ces graphiques en fonction de ces éléments.

Autres données que nous avons collectées au sein du bureau du directeur de la technologie, ce sont les ITHI, les indicateurs de santé de technologie des identificateurs. Cela a commencé en 2018 et cela nous a permis de surveiller un certain nombre d'identificateurs associés à la santé de l'écosystème des identificateurs. L'identificateur M2 en particulier relatif à l'utilisation malveillante des noms de domaine montre une tendance au fil du temps depuis le mois de janvier 2018 avec une utilisation malveillante par 10 000 domaines et compte les gTLD par bureau d'enregistrement qui représentent 50 % à 90 % des menaces à la sécurité reportées.

Si vous regardez le site web de l'ITHI, vous verrez que cela vous rappellera sûrement la situation du début des années 1990 avec des taux d'utilisation malveillante qui montrent par exemple dans le cas du hameçonnage que 10 des bureaux d'enregistrement représentent 90 % des menaces d'hameçonnage reportées. On voit ici 0,3 % pour les opérateurs de registre et 0,1 % pour les noms de domaine enregistrés pour les opérateurs de registre et bureaux d'enregistrement. Ce sont les informations provenant des bureaux

d'enregistrement, provenant de nos fournisseurs et ces données sont collectées et réunies dans une base de données au fil du temps parce que nous n'avons pas accès par l'intermédiaire du système DAAR aux informations liées aux noms de domaine individuels des bureaux d'enregistrement. Donc les informations des bureaux d'enregistrement, c'est quelque chose que nous utilisons comme indices et pas réellement comme une valeur précise. Les mesures relatives à l'ITHI, ce sont finalement des données brutes utilisées par DAAR, donc associées à ces informations fournies par les bureaux d'enregistrement. Diapositive suivante s'il vous plaît.

Autre projet que nous avons entrepris à l'OCTO et lié à l'utilisation malveillante du DNS, c'est le [DNSTICR], rapport de collecte et identification des menaces à la sécurité des noms de domaine qui a commencé en janvier 2020. L'objectif était de collecter des informations associées aux noms enregistrés pendant la pandémie. Et au début de la pandémie, il y a eu un certain nombre de rapports qui indiquaient qu'il y avait une croissance significative du nombre d'utilisations malveillantes de noms de domaine associés à la pandémie. Là, on regardait uniquement ce qui concernait le hameçonnage et les logiciels malveillants.

Et sur la période comprise entre mai 2020 et septembre 2020, on a collecté de manière systématique les données et effectué une analyse et on a découvert grâce à ce système que sur les 134 000 enregistrements détectés, environ 1,7 % montraient ou donnaient une indication suffisamment sûre de comportement malveillant. Diapositive suivante s'il vous plaît.

Si on regarde maintenant les données sur la période de juin à septembre 2020, 80 000 domaines liés à la pandémie ont été enregistrés et 170 ont donné lieu à des rapports qui ont été envoyés aux bureaux d'enregistrement liés à ces domaines concernant des risques. Cela indiquait que les noms de domaine avaient été enregistrés dans le système des noms de domaine et qu'il y avait au moins un rapport qui avait été trouvé concernant la liste de fournisseurs de réputation. Et lorsqu'on a regardé le site associé avec ces domaines, il y avait du matériel qui indiquait une menace contre la sécurité. Donc on a voulu minimiser le nombre de faux-positifs et d'environ 170 reportés, le 6 octobre, montraient que 87 n'existaient plus, ils avaient été retirés du système ; 56 ne satisfaisaient pas aux critères, il n'y avait plus de résolution du nom de domaine ou il y avait des menaces qui existaient ; 20 n'avaient pas de résolution, les enregistrements NS du serveur de noms ne répondaient pas ; et 7 étaient malveillants.

Je suis maintenant à votre disposition pour les questions. Je vous donne la parole, Thomas, s'il y a des questions.

THOMAS RICKERT : Merci beaucoup David.

Nous avons quelques questions. Nous allons voir si nous pouvons y répondre. Elizabeth [inaudible], j'espère que je prononce bien votre nom, demande : « En ce qui concerne les spams, est-ce que cela représente seulement les courriels ou est-ce que les spams

contiennent aussi d'autres formes d'utilisation malveillante technique tels que les logiciels malveillants ? »

DAVID CONRAD : Les logiciels que nous avons ne font pas de différence entre ces mécanismes de courriels malveillants et logiciels malveillants. Donc ce que vous voyez ici en ce qui concerne le spam est fourni par les fournisseurs de réputation. Dans le rapport du DAAR, dans le document de méthodologie, nous avons fait une liste des fournisseurs de réputation pour vous donner une idée des informations que nous avons collectées.

THOMAS RICKERT : Nous allons prendre deux questions de plus. Laura Schumann : « Ces diminutions ne paraissent pas liées au fait que les membres décrivent comme une augmentation de l'utilisation malveillante des domaines qui joue un rôle. Quel type de tendance est-ce qu'il y a ? Est-ce qu'on peut faire un parallèle ? Quelles sont les mesures de conformité qui seront prises ? Merci. »

DAVID CONRAD : En ce qui concerne la relation entre les courriels indésirables et les logiciels malveillants, les informations que nous avons recueillies à travers les fournisseurs de réputation, on a des personnes qui indiquent l'existence de certains spams avec des possibilités de hameçonnage qui vont montrer qu'il y a deux catégories différentes. Donc nous essayons de retirer les entrées redondantes de ce type,

mais cela n'est pas toujours possible. Il y a des cas dans lesquels ces noms sont dupliqués. Les informations que nous recueillons, nous ne les modifions pas. Ce sont les informations que nous agrégeons avec nombre de fournisseurs différents. Et on a des statistiques différentes concernant l'utilisation malveillante du DNS et les menaces dans ce sens. Donc il serait intéressant de savoir quelles sont les données qui sont utilisées pour fournir ces informations. Nous pouvons travailler avec le système DAAR pour voir comment incorporer ces séries de données dans le système DAAR et dans d'autres systèmes utilisés dans ce sens.

En ce qui concerne la deuxième question, je dirais que le nombre absolu d'opérateurs de registre ou de bureaux d'enregistrement représente 90 % et ils doivent être compris dans un contexte dans lequel il ne serait pas surprenant qu'il y ait une corrélation solide entre le nombre total d'enregistrements et le nombre d'utilisation malveillantes de ces enregistrements.

Si vous regardez les données non normalisées au niveau des opérateurs de registre et des bureaux d'enregistrement qui ont le plus grand nombre d'enregistrements, on a le plus grand nombre d'utilisations malveillantes de domaines. Il vaut mieux analyser tout cela dans le contexte des nombres normalisés comparés au nombre d'enregistrements. Lorsqu'on regarde ces chiffres, il est moins évident et on ne constate pas aussi facilement quels sont les mauvais acteurs.

THOMAS RICKERT : Je pense que nous allons passer au prochain orateur. Nous allons entendre maintenant Jeff. Et si vous voulez, vous pouvez aller dans l'onglet Q&A et poser des questions. Ensuite, pour les questions auxquelles nous pourrons répondre, nous y répondrons à la fin de la séance. Je pense que c'est une bonne manière de continuer.

Nous allons maintenant donner la parole à Jeff Bedser, qui travaille avec iThreat et qui travaille dans le groupe de travail d'utilisation malveillante du DNS SSAC.

JEFF BEDSER : Bonjour à tous. Je suis Jeff Bedser. Je vais indiquer que je vais représenter l'effort du groupe de travail du SSAC réalisé il y a un an.

Il y avait une charte difficile. Nous avons travaillé sur l'utilisation malveillante du DNS et nous avons travaillé sur ce type de problèmes avec un document qui n'a pas encore été publié et qui devrait être publié dans les semaines à venir. Nous voulions d'abord laisser passer d'abord la réunion de l'ICANN69. Une fois que ce processus sera terminé, nous présenterons ce travail. Prochaine diapositive.

D'abord, je voudrais m'assurer qu'il soit clair qu'une des choses qu'a fait le SSAC dans ce travail est d'inviter des personnes qui sont à l'extérieur du SSAC et qui ont participé à ce travail. Nous avons des personnes du groupe des parties prenantes, différents experts, différentes connaissances pour mieux comprendre les problèmes politiques, les problèmes techniques. Excusez-moi.

Nous avons un groupe de personnes qui sont à l'extérieur du SSAC qui nous ont offert leurs connaissances dans le domaine de l'utilisation malveillante du DNS, des personnes de différents bureaux d'enregistrement et des opérateurs de registre qui ont travaillé avec nous.

Une des choses dont a parlé David Conrad concernant les données d'utilisation malveillante, il y a des mesures qui existent pour certains jours, mais le problème que l'on a concernant l'utilisation malveillante du DNS est que chaque heure, chaque jour, il y a des utilisations malveillantes de domaines qui continuent à exister avec davantage de victimes, de pertes, etc. David l'a bien présenté dans son travail. Et tout cela est associé à l'utilisation malveillante du DNS.

Mais si l'on regarde les rapports qui existent, on travaille avec les forces de l'ordre, mais sans aucun doute, on ne peut pas attendre l'arrêt de cette utilisation malveillante du DNS parce que le cyberdélit va continuer à exister. C'est quelque chose de très difficile de freiner. Le problème ici que l'on affronte, c'est que la confiance des utilisateurs finaux envers internet au niveau commercial, au niveau personnel, au niveau des différentes activités que les personnes réalisent sur internet, implique une confiance dans le système, dans les fournisseurs de service. Et le rapport qui va être publié bientôt aborde la question de la méthodologie nécessaire pour réduire l'utilisation malveillante du DNS et établir des meilleures pratiques avec des coopérations entre les différents groupes.

Il faut se souvenir que les parties contractantes de l'ICANN représentent la totalité du système du DNS qui est utilisé. Et il y a d'autres fournisseurs d'hébergement de système de fourniture de contenu qui appartiennent à cette structure et qui forment cet écosystème dans sa totalité. Prochaine diapositive.

Les points clés ici de ce document sont les suivants. Encourager des normes de définition de ces utilisations malveillantes ; nous essayons de redéfinir cette définition et nous sommes partis d'une définition qui existait et qui était suffisamment bonne pour décrire le problème. Lorsque l'on aborde ce problème, on a une série d'aspects qui nous permettent d'avancer.

Le prochain point serait de déterminer le premier point approprié de responsabilité pour la résolution de ces problèmes d'utilisation malveillante. Chaque type va avoir ses caractéristiques et peut-être qu'à certains niveaux, au niveau de l'hébergement ou autres, à différents endroits dans l'écosystème, il va y avoir un endroit où on pourra lutter de manière plus appropriée contre cette utilisation malveillante.

Ensuite, il faut trouver les meilleures pratiques pour déployer les normes de preuve et c'est quelque chose de plus compliqué parce qu'ici, il y a différents prérequis, différentes exigences pour prouver que quelque chose est vraiment problématique, qu'il s'agit d'une fraude, qu'il s'agit d'un délit. Mais s'il y a des normes qui prouvent que cet incident en particulier est quelque chose que l'on peut utiliser

pour démontrer qu'il y a une fraude, cela va nous permettre d'agir contre ce problème.

Ensuite, établir et mettre en œuvre des voies pour faire remonter ces informations liées à l'utilisation malveillante du DNS, c'est très important pour les différentes parties prenantes, les différents acteurs pour essayer de résoudre l'utilisation malveillante. Mais le fait est que parfois, vous ne savez pas exactement quel est le point d'entrée et qui a la responsabilité de résoudre cet utilisation malveillante. Les autorités chargées de l'application de la loi peuvent se tourner vers le fournisseur d'hébergement mais lui ne répond pas à ce contact. Et vous passez à la partie prenante suivante pour essayer de réduire là encore le nombre de victimes d'utilisation malveillante du DNS.

Ensuite, déterminer un délai raisonnable pour entreprendre des actions, parce que pour l'heure, la plupart des parties répondent dans un délai de 24 heures. Donc si une partie prenante répond et qu'on la contacte à trois reprises, cela peut prendre 72 heures. Donc il faut déterminer un délai raisonnable pour entreprendre des actions et cela va permettre de résoudre également le délai dans lequel ce domaine sera victime de cette attaque.

Il y a beaucoup d'entités commerciales et d'entités à but non lucratif qui détectent des utilisations malveillantes et qui le rapportent. Mais une autre tendance intéressante qu'on a notée dans notre groupe de travail, c'est que le nombre d'entreprises qui font rapport et état d'utilisations malveillantes, ce sont de plus en plus des entreprises spécialisées, techniques qui se spécialisent justement dans ce

domaine de détection de l'utilisation malveillante des noms de domaine. Donc notifier, cela aiderait beaucoup.

Créer un mécanisme également pour la disponibilité des informations de contact en vue de l'atténuation de l'utilisation malveillante du DNS. Cela aussi, c'est très important à la lumière du RGPD et il s'agit des entités qui sont différents points d'entrée dans les noms de domaine. Parfois, ce sont des informations qui sont difficiles à trouver, parfois, il n'y a pas de mécanismes qui permettent d'avoir accès à ces informations. On ne sait pas à qui s'adresser pour trouver les informations de contact du nom de domaine.

Et enfin, créer un mécanisme pour assurer une qualité raisonnable des informations de contact pour atténuer l'utilisation malveillante du DNS.

J'espère, je vous le disais, que ce rapport sera disponible pour l'ensemble de la communauté dans les prochaines semaines. Et j'attends avec impatience vos commentaires et retours d'information. Et sans plus attendre, Thomas, je vous recède la parole.

THOMAS RICKERT : Merci beaucoup Jeff. Rien à redire par rapport au fond de ce que vous avez dit. Vous vous en êtes tenu aux 10 minutes qui vous étaient réservées, donc très bon travail.

Je vois que dans l'onglet Questions et réponses, ce sont des questions qui s'adressent à David Conrad. Donc si vous avez des questions à l'attention de Jeff, n'hésitez pas à les inscrire dans l'onglet Q&A et on

va faire avec Jeff comme on l'a fait avec Dave. Si vous voyez des questions sur l'onglet Q&A, essayez d'y répondre directement, ce qui va nous permettre d'avancer au prochain intervenant, à savoir Mason Cole.

Mason Cole fait partie du groupe des représentants des entités commerciales. Et il va nous parler du point de vue du groupe des représentants des entités commerciales. C'est à vous.

MASON COLE : Merci beaucoup Thomas. Vous m'entendez bien ? Très bien.

Bonjour, bon après-midi, bonsoir à tous. Je vais commencer cette présentation. Je ne suis pas sûr d'avoir besoin des 10 minutes qui m'ont été allouées, mais on va voir. Merci.

Nous nous retrouvons ici de nouveau à parler de l'utilisation malveillante du DNS et comme Jeff et d'autres l'ont dit, il s'agit d'un problème qui ne semble pas disparaître et ne va probablement jamais disparaître. Et à intervalle régulier, on voit que c'est quelque chose qui est magnifié par des événements externes, comme l'épidémie de la covid-19, des catastrophes naturelles, des troubles civiles, entre autres. Et le dénominateur commun ici, c'est que le DNS est utilisé à des fins malveillantes ou illicites. Et on pourrait continuer à parler de cela, mais aussi aborder les solutions productives et réellement essayer de faire quelque chose par rapport à l'utilisation malveillante du DNS de manière concrète.

Dans les statistiques qu'on a vues, il semblerait qu'il suffit de chercher toutes les informations en ligne par rapport à l'utilisation malveillante du DNS. Mais les statistiques les plus récentes publiées avant le rapport SSAC – et cela a été publié il y a quelques jours à peine – nous montrent que pendant cette période d'étude entre le 1er juin 2020 au 31 juillet 2020 – et cette étude s'est concentrée sur le hameçonnage – ce rapport a démontré 99 000 noms de domaine uniques dans 439 TLD et 414 bureaux d'enregistrement. Donc le problème de hameçonnage existe, l'ampleur exacte est inconnue mais en tout cas, on sait que ce problème est sous-estimé.

Ce que l'on sait au SSAC, c'est que l'utilisation malveillante du DNS et la cybercriminalité qui en résulte continuent à faire des millions d'utilisateurs de l'internet des victimes, donc sape la confiance des utilisateurs finaux vis-à-vis de l'internet, y compris du DNS. Or, c'est le socle de l'internet, que ce soit pour les relations personnelles, commerciales, non commerciales ou autres. Donc il est important d'avoir cette confiance, que ce soit à des fins commerciales ou non commerciales. Diapositive suivante s'il vous plaît.

Les statistiques et ce sur quoi on devrait se mettre d'accord. Je pense qu'on peut tous apporter notre point de vue sur cette question ; c'est ce qu'on a fait. Et je crois qu'on en est à quatre séances déjà sur cette thématique. L'utilisation malveillante du DNS peut être à la hausse ou à la baisse en fonction de la source de données que vous utilisez. Donc ce qui se passe, c'est qu'il y a un impact sur la confiance de l'internet, donc on doit apporter une solution fondée sur les données. Et c'est ce dont je vous parlais : on a la possibilité d'être plus proactifs et d'agir

de manière plus déterminée pour lutter contre l'utilisation malveillante du DNS.

Et il y a un argument ici au sein de l'ICANN par rapport au fait de savoir comment aborder cette question de l'utilisation malveillante du DNS. Ce n'est pas une guerre qu'on devrait se lancer les uns contre les autres. Il suffit simplement de s'en prendre aux mauvais acteurs.

Donc des progrès ont été effectués, comme d'autres avant moi l'ont dit. Et j'aimerais une fois de plus saluer le cadre volontaire mis en place par les opérateurs de registre et bureaux d'enregistrement depuis le début de l'année me semble-t-il ou peut-être l'année dernière, qui a eu un impact mesurable sur l'utilisation malveillante du DNS. Et on devrait saluer cela. Donc j'aimerais féliciter les parties contractantes qui ont fait un travail à ce niveau-là. Diapositive suivante s'il vous plaît.

Vous voyez qu'il y a des progrès qui ont été faits mais dans certains domaines, aucun progrès n'a été fait. Les cadres volontaires, c'est une très bonne chose, mais ils ne sont pas totalement inclusifs. On sait qu'il y a huit à 10 mauvais acteurs et en général, on sait où ils se cachent, ces mauvais acteurs. Donc ce serait utile de faire quelque chose par rapport à ces mauvais acteurs pour essayer de faire quelque chose par rapport à l'utilisation malveillante du DNS en dehors de ces cadres volontaires.

Revenons en arrière à Montréal. L'année dernière, lorsqu'on a offert un plan par rapport à l'utilisation malveillante du DNS. Je voulais rappeler l'intervention d'Elliot Noss de Tucows qui me paraît

particulièrement intéressante. On a besoin de traiter la question qui se trouve face à nous. Si la conformité peut identifier de manière efficace le fait qu'il y ait des éléments spécifiques dans le contrat qui nous aident à appliquer très clairement et à gérer et traiter les mauvaises actions dont on connaît l'existence, parlons-en. Et pourquoi je voulais rappeler cette intervention ? Parce que là encore, c'est une solution proactive qu'on peut apporter ici. Et il suffit d'utiliser des outils qu'on a déjà entre les mains puisqu'on a déjà identifié les mauvais acteurs. Et cela, c'est ma dernière diapositive.

À n'en pas douter, on ne va pas pouvoir arriver en haut de l'Everest en une journée. De la même manière, on a l'opportunité de s'attaquer à la question de l'utilisation malveillante du DNS de manière progressive. Et voilà les idées que je suggérais pour y parvenir.

D'abord, faire un tri par rapport aux résultats qu'on peut obtenir le plus facilement et qui créent les principaux problèmes dans l'espace des noms puisqu'on a les moyens.

Il y a les opérateurs de registre et bureaux d'enregistrement qui sont « propres » et l'organisation ICANN a l'opportunité d'être proactive par rapport à sa fonction de conformité. Et j'aimerais en appeler ici aux parties contractantes pour qu'elles se montrent proactives. Et d'ailleurs, le rapport indique bien qu'il faut mettre en place une prévention avant que ces activités aient lieu. Et ensuite, plutôt que d'avoir une plénière par conférence, il faudrait peut-être avoir des discussions plus approfondies et des rapports d'avancés pour voir ce qui se passe au sein de la communauté.

Thomas, je vous l'ai indiqué, c'était ma dernière diapositive donc je vous cède la parole.

THOMAS RICKERT : Merci beaucoup Mason.

On a deux questions qui s'adressent à vous. Je vais suggérer de répondre à ces deux questions avant de passer à l'orateur suivant. Et si vous pouvez être bref dans votre réponse, tant mieux.

Première question : « Par rapport au répertoire, est-ce que vous pouvez nous donner des détails par rapport au hameçonnage et personnes qui se cachent derrière le hameçonnage avec nombre d'utilisations malveillantes ? Est-ce que ces chiffres restent les mêmes ? »

JEFF BEDSER : Merci de cette question, Luke. Je vais essayer de répondre par écrit à cette question, parce que cela va me prendre un petit peu de temps pour répondre à cette question. Est-ce que je peux le faire par écrit ?

THOMAS RICKERT : Oui, bien sûr.

Je vois qu'il y a d'autres questions qui n'ont pas reçu de réponse. En tout cas, on y répondra par la suite.

Et je vois que les questions ont été publiées pour que tout le monde les voie. Donc si vous publiez une question, vérifiez si votre question a déjà reçu une réponse ou pas pour qu'on évite les doublons.

Ensuite, question suivante... Pardon, prochain intervenant, Chris Lewis-Evans du groupe de travail du GAC sur la sécurité publique et qui représente l'agence nationale de lutte contre la criminalité du Royaume-Uni.

CHRIS LEWIS-EVANS : Merci beaucoup Thomas.

Tout d'abord, diapositive suivante s'il vous plaît, pourquoi on parle de l'utilisation malveillante du DNS ? Mason vient d'en parler, il y a un certain nombre de séances organisées sur cette thématique. Pourquoi on en parle ? En raison de l'impact de l'utilisation malveillante sur l'utilisation de l'internet.

Je vous ai indiqué ici cinq statistiques qui vous indiquent différentes choses. Le centre des réclamations ou des plaintes déposées par rapport à la cybercriminalité du FBI a reçu 467 361 plaintes en 2019, ce qui représente 1 300 plaintes par jour. Et vous voyez ici les pertes, 3,5 milliards $. Dans tout l'internet, ce sont des individus, des entreprises ; tout le monde est concerné, tout le monde est touché.

Au Royaume-Uni, d'après nos statistiques nationales, on a enregistré que 85 % des fraudes qui ont été dénoncées l'ont été faites de manière cybernétique, en utilisant internet donc. Si vous regardez par exemple les rançons logiciels au niveau mondial, cela a un impact très élevé et

d'une année à l'autre, on constate une augmentation de 715 %. Donc ce ne sont pas seulement des pertes au niveau financier, c'est aussi des personnes qui, à cause de ces violations de données, vont présenter des plaintes. Donc on a ces violations de données personnelles qui représentent le hameçonnage et l'utilisation malveillante du DNS et qui sont attribuées à ce type de problème au Royaume-Uni, comme Mason l'a dit tout à l'heure. Prochaine diapositive.

Comme cela a été mentionné dans le chat, il y a une série de domaines dans lesquels on peut affronter les problèmes d'utilisation malveillante du DNS. L'ICANN va se concentrer sur les bureaux d'enregistrement et les opérateurs de registre, bien sûr, mais il faut aussi affronter tout cela à travers une réponse qui nous permettrait de travailler dans l'ensemble de l'écosystème de l'internet, les fournisseurs de service internet. C'est un grand environnement dans lequel nous travaillons et nous avons vraiment besoin de quelque chose qui nous aide à affronter tous ces types d'utilisation malveillante et au bon endroit.

Je vais vous montrer ici un système qui va nous permettre un petit peu de faciliter cela. D'abord, l'ICANN, quand on parle de l'utilisation malveillante du DNS, il faut souligner le travail proactif qui a été fait qui est d'une grande importance. Nous avons besoin de mettre en place des mesures proactives pour que cela puisse donner des résultats. L'ICANN va faciliter ce processus de travail dans l'environnement à travers les groupes de parties prenantes. Prochaine diapositive.

Ici, plusieurs solutions. Que pouvons-nous faire ? Nous pouvons travailler avec l'ICANN. J'ai eu déjà plusieurs réunions avec le groupe des opérateurs de registre et autres parties prenantes. J'ai tiré des connaissances des plaintes réalisées en cas d'utilisation malveillante. Mais ce n'est pas le même processus que les forces de l'ordre ou autres services de sécurité utilisent, donc nous avons des preuves que certaines personnes essayent d'affecter certains domaines, certaines suspensions. Ce n'est pas toujours très clair ce qu'il faut modifier dans le domaine de l'utilisation malveillante du DNS. Il y a différents types de contenu et parfois, les premières réponses ne sont pas les bonnes.

Qu'est-ce qui arrive si on ne met pas en place des actions ? Comment on peut trouver des moyens d'escalader ? Comment on passe d'un hébergement web ? Comment retirer certains contenus ? Lorsqu'un bureau d'enregistrement ne répond pas, que faire ? Et avec ces mécanismes qui sont en place, nous pouvons avancer et augmenter le niveau de la barrière pour mettre en place des actions proactives et pour rendre la vie de ces délinquants plus compliquée.

Vous savez qu'il y a toujours des systèmes qui vont parvenir à leur objectif. On essaye d'être réactif. Il y a des points clés. Tous les processus que nous avons doivent être mis en place au bon moment et réalisés de manière efficace.

Je crois qu'il est aussi très important qu'on ne dise pas seulement : « Donnez-nous les données. » On va mettre en place des techniques et des mesures appropriées. Il faut aussi qu'il y ait des accords qui vont nous permettre de travailler de manière appropriée, parce que nous

ne voulons pas contacter un bureau d'enregistrement ou un opérateur de registre directement en cas d'incident. Nous voulons avoir un cadre de travail avec des accords, un processus pour savoir quel type d'actions réalisées, comme cela a été dit tout à l'heure. Il y a des normes qui sont nécessaires pour prouver. Tout cela est très utile pour réduire ce type de délits.

Pour moi, je pense qu'il y a encore beaucoup de choses à faire. Il y a eu des mesures proactives qui ont été très efficaces mais ici, lorsque l'on parle de l'utilisation malveillante du DNS et lorsque l'on veut réduire le nombre de domaines qui font ce type de délits, il nous faut être conscient qu'il doit y avoir des mesures organisées pour lutter contre ce type de délits.

Merci.

THOMAS RICKERT : Merci beaucoup Chris.

Je vais lire la question de Maxime [inaudible] : « Il y a beaucoup d'appels concernant une approche proactive. Est-ce que vous pensez que les RIR sont concernés aussi dans ce processus ? »

CHRIS LEWIS-EVANS : Oui, je dirais qu'ils jouent un rôle important dans cette partie de l'écosystème. On travaille dans ce domaine et je pense que c'est une question qui est très importante.

THOMAS RICKERT : Une autre question de Maxime : « Il y a des rapports proactifs. Comment on peut expliquer les actions à mettre en œuvre ? Qu'est-ce qui a été fait pour les domaines en question ? »

CHRIS LEWIS-EVANS : Il est très difficile de prédire ce qui va avoir lieu dans ce domaine des délits et ce qu'on peut faire. Mais je dirais que si nous avons des systèmes en place qui peuvent affronter ce type de problèmes, ce sera une mesure proactive. Donc avoir les systèmes adéquats en place va nous permettre de mettre en place des actions. C'est une bonne approche. Il va y avoir beaucoup d'activités des parties contractantes et le cadre de lutte contre l'utilisation malveillante du DNS, tout cela. Donc je crois qu'il y a beaucoup de choses qui peuvent être faites dans ce sens de manière proactive pour annuler ce type d'utilisation malveillante du DNS. De tout façon, nous ne pouvons pas prédire tout cela.

THOMAS RICKERT : Je crois que c'est quelque chose dont nous pouvons discuter plus tard avec les différents panelistes.

Avant de passer au prochain orateur, j'ai une question. Vous avez parlé dans une de vos diapositives de 85 % de cas de fraude. Quand on parle d'utilisation malveillante du DNS, est-ce qu'on parle de ce type de choses ?

CHRIS LEWIS-EVANS : Non, ce n'est pas seulement l'utilisation malveillante du DNS. Il y a aussi des questions de courriels indésirables. Quand on parle de définition de l'utilisation malveillante du DNS, c'est plus compliqué. La discussion ici, comme Jeff l'a dit, c'est qu'est-ce que l'utilisation malveillante du DNS ? Il y a d'autres mécanismes qui sont concernés ici qu'il faut comprendre quand on analyse cette question.

THOMAS RICKERT : Merci Chris.

Il y a une question de Monica [Amat]. Il y a eu des plaintes liées à la diversité de genre, donc nous allons prendre cette question de Monica : « Est-ce que vous pouvez nous donner des détails sur 60 % de violations de données rapportées qui sont attribuées au hameçonnage ? Est-ce que vous pouvez nous donner des détails sur les sources et le type d'actions ? »

CHRIS LEWIS-EVANS : Oui. Ce sont des données qui ont été publiées. Je peux vous donner ces détails dans le chat.

THOMAS RICKERT : Merci beaucoup.

Nous allons passer au dernier intervenant, James Bladel de GoDaddy qui va prendre la parole. James, allez-y.

JAMES BLADEL : Merci Thomas. Est-ce que vous m'entendez ?

THOMAS RICKERT : Oui, on vous entend. Allez-y.

JAMES BLADEL : Bonjour ou bonsoir à tous. Merci de m'avoir inclus dans cette discussion.

Un des avantages d'être le dernier ici est d'avoir entendu les commentaires et ce que les autres intervenants ont dit ; comme cela, je ne répèterai pas ce qui a déjà été dit. Je ne voulais pas présenter la perspective des parties contractantes parce que je pense qu'à mesure qu'on avance dans les diapositives, cela correspond un petit peu à ce qui a été dit auparavant.

Je dirais qu'en général, l'utilisation malveillante du DNS en ligne, comme cela a été dit, est un grand défi pour notre secteur et une priorité pour les parties contractantes. Cela est indiqué par tous les investissements qui ont été faits jusqu'à maintenant dans ce domaine. Et les résultats des parties contractantes et des opérateurs qui travaillent avec l'ICANN ont démontrés que l'utilisation malveillante du DNS en général est atténuée à un certain niveau. Mais je dirais qu'il nous faut reconnaître les distinctions entre l'utilisation malveillante du DNS, l'utilisation malveillante de contenu et d'autres types d'utilisation malveillante qui sont spécifiques au DNS. Et je pense que cela est lié aux remarques faites par Thomas au début. Ici, l'ICANN a

un rôle important à jouer dans ce domaine contraint tel qu'indiqué dans ses statuts constitutifs. Prochaine diapositive.

Si on part de cela, la mission de l'ICANN est de préserver la sécurité et la stabilité du DNS, mais la plupart de ces utilisation malveillantes du DNS, particulièrement les courriels indésirables, les fraudes et autres types réalisés en ligne, dépendent du contenu. Et c'est là qu'on parle des responsabilités de l'ICANN. Je dirais qu'on peut aussi parler de la capacité des bureaux d'enregistrement et des opérateurs de registre à atténuer les utilisations malveillantes de contenu. Nous parlons souvent de cette option nucléaire et de la capacité des bureaux d'enregistrement ou des opérateurs de registre à retirer certains noms de domaine. Ce n'est pas approprié en cas d'utilisation malveillante ou de contenu lorsqu'il y a une fraude. Par exemple, lorsque l'on constate cela sur une page de Facebook, on ne peut pas annuler Facebook. C'est la même chose pour eBay, on ne peut pas suspendre le site ebay.com. Nous avons certaines options, mais seulement un niveau d'options. Heureusement, la plupart des bureaux d'enregistrement et des opérateurs de registre se trouvent dans différentes parties de l'écosystème. Par exemple, on a un bureau d'enregistrement ou opérateur de registre avec différents systèmes, différents outils que l'on peut utiliser lorsque les utilisations malveillantes sont détectées.

Une des raisons pour lesquelles les parties contractantes disent que seulement une portion du problème de l'utilisation malveillante du DNS apparaît, nous savons, au niveau du secteur, qu'il y a différents

efforts réalisés à l'extérieur de l'ICANN aussi pour affronter ce type d'utilisation malveillante.

En septembre de l'année dernière – et d'ailleurs, c'était juste avant qu'on se voie pour la dernière fois à Montréal – les opérateurs de registre et bureaux d'enregistrement ont lancé le cadre de l'utilisation malveillante du DNS. L'objectif était justement de normaliser certaines définitions et des normes en termes d'attentes dans le domaine des actions. Et je pense que Jeff en a parlé en parlant du rapport SSAC, identifier qui était les parties responsables pour telle ou telle situation et quelles étaient les actions d'atténuation typiques.

Pour l'instant, nous avons plus de 50 signataires qui ont souscris à ce cadre. Et comme Mason l'a dit, cela a un impact puisque cela pousse un petit peu les opérateurs de registre ou bureaux d'enregistrement qui étaient moins capables de faire face à ce problème et les a mieux armés pour y répondre. Et hier, ces mêmes signataires ont lancé une mise à jour un an après la signature et après le lancement de ce cadre. Et ce document contient certaines statistiques, certaines tendances, mais pas forcément avec des statistiques et des tendances, mais avec des informations, des tendances et peut-être moins de chiffres.

Et au mois d'avril ou de mai 2019, le réseau politique de l'internet et de la juridiction a publié un document en mettant en exergue les défis et les pratiques dans le domaine de l'atténuation de l'utilisation malveillante du DNS. Et cela ressemble beaucoup au cadre de l'utilisation malveillante du DNS en incluant quelques éléments que nous n'avions pas nous inclus dans notre cadre.

Outre l'utilisation malveillante du DNS, s'agissant du contenu, il y a beaucoup d'associations, d'alliances, de coalitions de l'internet, de groupes de travail, appelez-les comme vous le voulez, qui ciblent spécifiquement des catégories d'utilisation malveillante comme le courriel indésirable, le contre-terrorisme, la pornographie infantile, etc. L'objectif ici, parce que vous ne voyez pas forcément l'action entreprise dans ce domaine, cela ne veut pas dire qu'il n'y a pas de travail qui est effectué. De fait, beaucoup de parties contractantes ont participé à ces autres organisations, comme [inaudible] et d'autres. Diapositive suivante s'il vous plaît.

État actuel des choses. Cette année, vous le savez, cela a été une année particulière. Le monde entier a dû s'adapter au mode virtuel en réponse à la pandémie de la covid-19. Et si l'on parle spécifiquement des petites entreprises, tout le monde a dû s'adapter aux livraisons à domicile des repas, l'école à la maison. Les organisations civiques et politiques ont toutes dû s'adapter au format virtuel et c'est le cas de l'ICANN aussi. Pourquoi est-ce que je le dis ? Parce que notre secteur de l'industrie a énormément contribué à cela puisque c'était des tendances qu'on voyait déjà se dessiner, mais la pandémie de la covid-19 a accéléré un petit peu cette adaptation en quelques mois à peine. Et nous espérons qu'une fois que cette pandémie sera surmontée, on sera un petit peu plus souple et qu'on va pouvoir rebondir après cette transformation.

Mais on ne devrait pas être étonné de voir que la plupart des délinquants et des mauvais acteurs et opportunistes se sont transformés aussi, ils se sont aussi adaptés et ont donc fait évoluer

leur approche en termes d'attaques et ont suivi l'endroit où se trouvaient leurs victimes. Et ils sont passés d'une économie physique à une économie virtuelle ou cybernétique.

Mais cela étant dit, les données ne nous montrent pas qu'on en soit à la fin du monde, loin de là. Et je pense que cela nous renvoie un petit peu aux statistiques que nous montrait David en début de séance puisqu'on voit dans notre secteur de l'industrie une certaine résurgence dans le nombre de cas de hameçonnage et on a vu certains PIC au printemps, au début de l'été aussi. Mais d'une manière générale, je pense qu'on va vu une croissance modeste et je n'ai pas de statistiques centralisées, ce sont des statistiques qui nous viennent de GoDaddy, mais en tout cas, rien ne ressemble en termes d'ampleur et rien n'indique un nouveau type d'attaques qui serait élaboré.

Ensuite, GoDaddy est en train de traiter 2 000 cas de hameçonnage par jour. Ce sont juste des rapports parce que certains de ces cas ne sont pas forcément des incidents. Ce sont des cas où parfois, moins de 8 % ou parfois moins de 3 % de ces rapports sont recevables. Il y a beaucoup d'informations, c'est difficile d'être spécifique par rapport à ces incidents. Et peut-être que c'est là qu'il faudrait travailler en coopération avec l'OCTO pour essayer de se concentrer sur les problèmes légitimes. Diapositive suivante s'il vous plaît.

Ce n'est pas forcément lié à la question qui nous occupe aujourd'hui, mais cela fait partie de la même thématique : le problème des escroqueries, des campagnes de fraude associées à la pandémie. Bien entendu, cela a fait la une des journaux dans la première partie de

l'année et je pense que Mason a fait référence aux PIC qu'on a vus au mois de mars et en avril lorsque tout le monde était confiné. Et je pense qu'ici, la conclusion, c'est qu'il s'agissait d'attaques concentrées sur le contenu et qui n'étaient pas particulièrement nouvelles. Elles étaient nouvelles dans le sens où elles essayaient de tirer partie des principales informations ou nouvelles de la journée, mais en fait, il s'agissait des mêmes attaques de hameçonnage qu'on connaît depuis des années maintenant.

Dans notre cas par exemple, chez GoDaddy, on n'a pas eu le sentiment qu'il fallait s'arracher les cheveux pour essayer de mettre en place de nouvelles compétences ou une nouvelle politique. Non, on a considéré qu'on était suffisamment bien armé pour faire face à ces campagnes de fraude. Et là encore, beaucoup d'efforts d'atténuation ont été faits au niveau de l'hébergement des sites web.

Et je pense qu'il y a eu des questions et un commentaire de Chris et de Mason par rapport aux mesures proactives à mettre en place. On voit beaucoup de propositions et de pression de la part des uns et des autres pour bloquer la covid-19, qu'elle ne soit pas incluse dans le DNS, parce que cela va seulement servir à être utilisé à mauvais escient. Donc je comprends bien l'objectif de cette solution mais en fait, les choses sont beaucoup plus compliquées que cela dans les faits. La plupart des noms de domaine dommageables qu'on voit ne font pas une référence explicite au coronavirus ou à la covid-19. Et inversement, on voit beaucoup d'autorités de santé publique et de gouvernements locaux qui utilisent ces noms de domaine pour donner des instructions officielles ou des mises à jour officielles en utilisant

ces mêmes liens. Donc bloquer des chaînes dans le DNS pour régler le problème, je pense que c'est un peu limité. Même si c'est tentant comme solution, ce n'est pas une approche qui soit ni efficace ni acceptable en termes de faux-positifs ou d'effets collatéraux. Diapositive suivante s'il vous plaît.

Conclusion. Je pense que l'utilisation malveillante du DNS, c'est quelque chose d'important, mais notre rôle en tant que bureaux d'enregistrement, opérateurs de registre, et ICANN fait qu'on a plus d'outils à notre disposition pour régler cela. On pense qu'il est important à l'ICANN de faciliter les discussions au sein de la communauté, obtenir plus de points de vue différents au sein de la communauté sur cette question, faire des recherches aussi, collecter aussi des statistiques ; cela aide. Et vous ne serez pas surpris de m'entendre dire cela, mais il y a certaines hésitations par rapport à certaines parties contractantes par rapport au fait le lancer de nouveaux efforts dans ce domaine. Je pense que d'abord, il faut définir très strictement le problème et ce qui relève de la mission de l'ICANN et deuxièmement – et cela revient à la citation d'Elliot qui faisait partie de la présentation de Mason – s'assurer qu'on épuise tous les mécanismes des parties contractantes pour réduire notre action vis-à-vis des mauvais acteurs et voir si on met en place de nouvelles politiques. Sachant qu'il y a des méthodes qui ont marché, qui ont démontré qu'elles ont marché, pourquoi en créer d'autres ?

Voilà, j'en ai fini avec ma présentation, Thomas. Et merci de m'avoir invité et de votre attention.

THOMAS RICKERT : Merci James.

Nous avons une question qui vous est adressée. Je vais vous la lire. C'est de Mark Svancarek : « Question pour James. Est-ce qu'un accord de notifiant de confiance serait une bonne mesure d'atténuation ? »

JAMES BLADEL : Vous savez, je pense que c'est un bon moyen d'appliquer un filtre sur les faux-positifs et sur les rapports. Tout ce qu'on peut faire pour donner les moyens à nos équipes de se concentrer sur la menace en elle-même vaut le coût d'être exploré.

THOMAS RICKERT : Merci beaucoup.

Nous avons maintenant environ 17 minutes avant la fin de cette séance. Je vois que les questions dans l'onglet Q&A reçoivent une réponse de la part des membres du panel. Donc je vais laisser cela se dérouler pour ce qui concerne l'onglet Q&A.

Je vais revenir sur une question autour du format de ces séances plénières dont l'objectif serait de produire des recommandations ou des résultats concrets ; c'est ce que disait Mason. Donc je pense qu'on a tous entendu les mêmes présentations, mais je ne sais pas si on a tous retenu la même chose de ces présentations. Donc je vais essayer de revenir sur certains points sur lesquels je l'espère on sera d'accord et sur lesquels j'espère on va pouvoir travailler.

Le premier point sur lequel j'aimerais que le public ou les membres du panel réagissent, c'est la définition de l'utilisation malveillante du DNS, parce que les actions peuvent être actives ou proactives, mais dépendent énormément de qui prend ces décisions ou ces actions. Et une référence a été faite dans la présentation de Chris Lewis-Evans et dans celle de James Bladel au cadre de l'utilisation malveillante du DNS. Et cela a mis en exergue un certain nombre de points par rapport aux logiciels malveillants, par rapport aux réseaux zombie, par rapport au dévoiement et à la question de la fraude. Est-ce que ce serait une bonne idée – et cela, c'est une question à l'attention de Jeff – que vous et le SSAC puissiez travailler sur cette base puisque vous avez dit que vous travaillez sur une définition ? Je pense que ce serait une bonne chose pour tous d'avoir une compréhension commune de ce que constitue l'utilisation malveillante du DNS.

Et pour ceux qui posent encore des questions, n'hésitez pas à mettre vos questions sur l'onglet Q&A puisque le personnel de l'ICANN m'a indiqué qu'on ne va pas essayer, étant donné qu'on n'a plus beaucoup de temps, d'activer les micros du public. On va traiter les questions et les lire à haute voix.

Jeff, est-ce que vous pouvez répondre à cela ?

JEFF BEDSER : Je dirais qu'un cadre commun pour la définition serait une manière de résoudre le problème parce qu'à ce moment-là, nous pourrons lutter contre le cyberdélit. En fonction de tout cela, nous allons pouvoir le définir et affronter le problème. Je pense que c'est une composante

clé pour trouver les solutions contre l'utilisation malveillante du DNS, trouver une définition, savoir quel type de fraudes particulières, quel type d'événement contre le domaine va rentrer dans quelle catégorie.

THOMAS RICKERT : Est-ce que le SSAC a analysé la définition offerte par le document du cadre de l'utilisation malveillante du DNS ?

JEFF BEDSER : Merci Thomas.

Oui, nous avons travaillé sur tous ces points dans la section qui s'appelle définition.

THOMAS RICKERT : Est-ce que quelqu'un d'autre parmi les panelistes voudrait ajouter quelque chose pour donner votre avis à propos de ce qui vient d'être dit sur la définition de l'utilisation malveillante du DNS ? Est-ce que vous avez quelque chose à dire, est-ce que vous êtes d'accord ou pas ? Est-ce que vous pensez que ce rapport sur l'utilisation malveillante du DNS aborde correctement cette définition ? Si vous avez quelque chose à dire, dites-le. Si vous pensez que ces définitions ne sont pas correctes à votre avis, dites-le.

JAMES BLADEL : Je pense que c'est un bon départ. Je pense qu'on peut faire davantage de travail aussi, continuer à travailler là-dessus. Il y a des questions

dans la chat : Où on va à partir de là ? Comment on continue ? Comment est-ce que les prochaines réunions de l'ICANN vont aborder cette question ? On peut lancer quelques discussions sur la définition, voir un petit peu ce qui est dans le cadre de travail en fonction du SSAC et du rapport, ensuite inclure l'analyse de la raison pour laquelle il est approprié de la part de l'ICANN qui a un rôle quand même limité auprès des bureaux d'enregistrement et des opérateurs de registre, comment donc l'ICANN doit considérer ces définitions et quelles sont les réponses qui correspondent à quels groupes concernés. L'offre que l'on pourrait faire ici serait de trouver différents terrains d'accord.

THOMAS RICKERT : Merci beaucoup James.

MASON COLE : Merci.

Je voudrais reprendre un petit peu ce qui a été dit. Le cadre dans le rapport du SSAC est un bon départ pour une définition. Et ce que j'ai dit dans ma présentation, je pense qu'il n'y a pas encore de définition concernant l'action à réaliser et mettre en place contre ces types de délits. Alors je voudrais que la communauté comprenne cela. Le CSG et d'autres aimeraient voir l'ICANN mettre en place des actions claires. Et je pense que nous pouvons nous réunir, parler de l'utilisation malveillante du DNS, mais ici, ce que nous devons faire, c'est de passer à une étape d'actions concrètes ; c'est très important. La définition ne suffit pas.

THOMAS RICKERT : Merci.

JAMES BLADEL : Je pense ce dialogue peut être intéressant. En tout cas, Mason, je pense qu'il y a ici un point de divergence pour nous : c'est que si nous avons une définition, si nous comprenons mieux le problème et les responsabilités de chacun, nous pourrons mettre en place des actions. C'est important de le dire. Peut-être que je ne l'ai pas bien expliqué dans ma présentation, mais il n'y a pas d'absence de travail sur ce problème. C'est peut-être moins visible au sein de l'ICANN parce qu'il y a d'autres secteurs, d'autres compagnies ou d'autres groupes au sein de l'ICANN qui travaillent. Mais nous faisons des choses et nous faisons des choses en général.

MASON COLE : Je vous remercie, James. Je pense quand même qu'il y a des mauvais acteurs que l'on connaît. Et peut-être qu'il y a d'autres choses qui ont lieu sur la scène que les parties contractantes ne voient pas, mais je pense que vous pourriez avoir une approche plus proactive de l'utilisation malveillante du DNS.

THOMAS RICKERT : Parfait. Je crois que c'est ce qu'on attendait, une bonne interaction entre les panelistes ; c'est bien qu'elle ait lieu.

Je pense que personne ne peut considérer le travail politique comme une excuse pour ne pas mettre en place des actions. Les discussions qui viennent d'avoir lieu entre les parties contractantes indiquent que chacun fait un petit peu quelque chose. Chaque partie a un rôle crucial. Nous devons nous assurer que les opérateurs de registre et les bureaux d'enregistrement ont leur place dans cet écosystème et peuvent mettre en place des actions appropriées pour lutter contre ce type de problèmes. Par exemple, une association avec laquelle je travaille qui reçoit des plaintes du public en général, avant ce panel, j'ai contacté le directeur de ce panel pour lui demander ce qu'il préférait aller voir en cas de problème, les bureaux d'enregistrement ou les opérateurs de registre. Et ils m'ont dit qu'ils préféraient parler avec le responsable de l'hébergement parce que des fois, il y a des preuves à ce niveau-là et cela permet d'aller à la racine du problème. Donc je crois qu'il faut bien comprendre cela.

Il semble qu'il y ait des désaccords au niveau des statistiques maintenant. Certains disent que le nombre de problèmes diminue, d'autres au contraire, que c'est plus ou moins une tendance qui est plus ou moins la même. David, est-ce que vous voulez reprendre un petit peu ce qui a été dit dans la partie du chat et dans la partie des questions et des réponses ? Est-ce que vous pouvez nous faire un résumé des tendances concernant les statistiques ?

DAVID CONRAD : Je crois qu'on regarde différentes parties ici. Il y a des questions concernant ce qui est l'utilisation malveillante du DNS. Que mesurent

les personnes par rapport à cette utilisation malveillante du DNS ? Je dirais que la tendance que j'ai vue dans le chat concernant les indications reçues par différents groupes concernant les différents chiffres et les données qu'ils ont, je pense que ce serait intéressant d'avoir les données d'autres groupes. Nous essayons de collecter le plus grand nombre de données possible pour fournir des informations à la communauté, former ces discussions. Plus nous aurons d'informations, mieux nous comprendrons tout ce qui se passe, quelle est la réalité actuelle concernant l'utilisation malveillante du DNS. De mon point de vue, je dirais que les données que nous avons montrent dans le temps que l'utilisation malveillante du DNS diminue. D'autres disent que l'utilisation malveillante du DNS augmente. Il serait intéressant de voir quelles sont les données qui indiquent cela et quelles sont les données que les personnes considèrent pour dire ce type de choses et quelles sont les statistiques utilisées.

JAMES BLADEL : Je peux répondre ici ?

Certaines indications montrent que le problème n'est pas distribué de la même façon à travers le DNS et à travers internet. Par exemple sur les diapositives de David, il y avait des chiffres qui montraient des augmentations. On peut avoir des cas dans lesquels les niveaux ne changent et de temps en temps, il y a des augmentations. C'est peut-être les distinctions que nous avons constatées, c'est-à-dire que les chiffres ne sont pas différents, mais si on les regarde selon des angles différents, ces chiffres peuvent être analysés différemment.

THOMAS RICKERT : Merci beaucoup.

J'ai une autre question pour Chris. Maintenant que nous avons entendu David et James, peut-être parler des statistiques, parler des données qu'ils utilisent pour expliquer les statistiques, les résultats qu'ils ont, les actions constatées, les faits, etc. Est-ce qu'il y a des discussions au niveau des forces de l'ordre ? Est-ce que vous êtes en accord avec le secteur ? Est-ce que vous travaillez sur les mêmes bases factuelles pour expliquer ce type résultats ?

CHRIS LEWIS-EVANS : Les forces de l'ordre ont mis en place des changements ces dernières années pour travailler de manière plus transparente. Nous avons un rapport qui indique quelles sont les causes de tous ces changements. Et le FEI a élaboré un rapport parce qu'au sein de l'ICANN aussi, nous essayons de nous mettre d'accord sur des normes communes. Je pense que le travail doit être réalisé, il y a un travail qui doit être fait ici. Cependant, je dirais qu'il est aussi important d'utiliser les données que nous recueillons de manière transparente pour permettre à chacun de jouer son rôle dans l'écosystème.

THOMAS RICKERT : Il nous reste encore deux minutes. Je voudrais essayer maintenant de résumer ce qui a été dit.

Je crois que ce que nous avons entendu, ce sont beaucoup de commentaires. C'est tout à fait positif. Les panelistes étaient d'accord et même un petit peu au-delà pour dire qu'il serait bon d'avoir une définition commune du problème, des statistiques communes, des points de données communs.

Et il est clair aussi qu'on suggère que les problèmes devraient être accompagnés de preuves et de données indiquant une corrélation entre ce que l'on a et ces données, de façon à ce que les actions mises en place ne soient pas seulement anecdotiques.

Je voudrais aussi revenir à un point qui a été mentionné par Jeff dans sa présentation et il s'agit de la formation. Les utilisateurs finaux doivent être mieux éduqués pour lutter contre ce type d'utilisation malveillante du DNS. On a ici une combinaison de différentes actions qui peuvent permettre de remédier au problème et être utilisées par les différents acteurs à travers les parties contractantes, l'ICANN, les forces de l'ordre, etc.

Je crois que c'est un bon point de départ. Je n'ai pas participé au document de cadre de cette utilisation malveillante du DNS, mais je crois que les recommandations qui pourraient être recueillies à la base seraient que nous devons discuter de points tels que les différentes définitions des problèmes liés à l'utilisation malveillante du DNS. On ne doit pas réinventer la roue mais travailler sur ce qui a déjà été fait au préalable.

Je voudrais maintenant remercier les panelistes, le personnel de l'ICANN, le personnel technique qui nous a permis d'organiser cette

séance qui s'est si bien passée. Je voudrais aussi remercier tous les participants. Il est difficile de suivre des heures de réunions à distance sans avoir aussi le bon côté de la réunion qui est de rencontrer les gens dans les couloirs de boire un petit café entre chaque réunion. Donc je vous remercie.

Cette réunion est maintenant terminée.

[FIN DE LA TRANSCRIPTION]