ICANN82 | Forum de la communauté – GAC : discussion sur l'utilisation malveillante du DNS
Mardi 11 mars 2025 – 10h30 à 12h00 PST

NICOLAS CABALLERO Bonjour à tous. Nous vous demandons de prendre place. Nous allons bientôt commencer.

GULTEN TEPE OKSUZOGLU Bienvenue à cette discussion sur l'utilisation malveillante du DNS atténuation au GAC. Sachez que cette séance sera enregistrée et qu'elle sera régie par les normes de comportement de l'ICANN ainsi que par la politique anti harcèlement de l'ICANN.

Pendant la séance, les questions et les commentaires envoyés dans le chat seront lus à voix haute s'ils sont formulés de la manière attendue. Veuillez donner votre nom et la langue dans laquelle vous allez intervenir si vous parlez dans une langue autre que l'anglais. Parlez clairement et lentement pour permettre une bonne interprétation de vos propos et assurez-vous d'éteindre tous les autres dispositifs lorsque vous intervenez. Vous aurez accès à toutes les fonctionnalités de cette séance dans le menu de Zoom.

Ceci étant, je vais céder la parole au président du GAC, Nico Caballero. Nico.

NICOLAS CABALLERO

Merci Gulten. Bonjour à tous, bonsoir, encore une fois, suivant le cas. Bienvenue à cette séance sur l'atténuation de l'utilisation malveillante du DNS. Nous avons une liste fantastique d'intervenants. Nous avons Leticia Castillo de la conformité de l'ICANN. Nous avons Siôn Lloyd. Est-ce que je prononce bien votre nom? Il n'est pas encore là. Très bien. Nous avons Graeme de NetBeacon. Nous avons Reg Levy de Tucows. Nous avons Luc et Jeff. Bienvenue à tous.

Et, les responsables de thématiques du GAC, c'est Martina Barbero, de la Commission européenne et Tomonori du Japon. Nous avons une discussion intéressante sur les détails et les nuances de l'utilisation malveillante du DNS. C'est pour ceci sans plus attendre, je vais céder la parole à mon collègue distingué du Japon, Tomo. Tomo

TOMONORI MIYAMOTO

Merci, Monsieur le président Nico. Bonjour à tous et bienvenue à cette séance sur l'utilisation malveillante de DNS du GAC. Je suis Tomo du Japon et cette séance est également avec Martina de l'Egypte qui est avec nous en ligne et donc je suis japonais. Encore une fois, nous avons Leticia de la conformité de l'ICANN. Nous avons Sion de l'OCTO, nous avons Jeff du SSAC, nous avons Luc et Jeff de la CPH et Graeme de NetBeacon qui sont avec nous. Merci à tous.

Vous avez ici l'ordre du jour de la séance. Nous allons partager les réseaux du sondage du GAC sur l'utilisation malveillante du DNS et les mises à jour de la conformité contractuelle de l'ICANN. Nous allons parler du rapport INFERMAL et du rapport domaine Metrica. Nous allons également parler des étapes suivantes pour l'atténuation de l'utilisation malveillante du DNS.

Ensuite, je vais vous présenter brièvement certains points pour vous donner le contexte de cette séance sur l'utilisation malveillante du DNS. Comme vous le voyez, l'utilisation malveillante des DNS et son atténuation est une question importante. Nous avons déjà parlé avec le SSAC de la NCSG lors de séances précédentes sur ceci. Ceci est lié également avec la question de l'exactitude des données. C'est également lié avec les RA, les RAA. Les bureaux d'enregistrement et opérateurs de registre doivent réagir aux au signalement d'utilisation malveillante de DNS.

Il y a différentes compréhensions, différents contextes et démarches sur l'utilisation malveillante DNS, y compris les problèmes de cybersécurité. Certains pays travaillent sur les dangers en ligne. Il faut noter que la définition de l'utilisation malveillante du DNS dans les contrats de l'ICANN est claire et limitée. Donc, il s'agit de programmes malveillants, de réseaux zombies, d'hameçonnage, de dévoiement et de pourriels. Mais, il y a aussi différents types de mauvaises utilisations.

L'enjeu de l'utilisation malveillante du DNS est géré et donc il faut parler des différents travaux au sein de l'ICANN. Il faut également voir ce qui est fait en dehors de l'ICANN et partager les informations sur les différents travaux.

Pour certains d'entre vous vous rappelez certainement de ce diagramme qui nous donne toute la communauté décrite. Vous avez les contrats de l'ICANN et l'envergure de leurs applications. Il nous faut donc considérer la relation entre les contrats qui établissent les relations entre les différentes parties prenantes. Il y a la relation avec la communauté. Il y a aussi tout ce qui peut être fait en dehors des contrats de l'ICANN.

Ensuite, vous avez là un de nos travaux. Nous avons parlé lors de l'ICANN 81 d'Istanbul de ce qui pouvait être fait au sein de l'ICANN. Nous avons eu une présentation d'information sur la conformité. Nous avons parlé avec les parties prenantes ainsi qu'avec la CPH. En janvier, février, nous avons effectué un sondage sur l'utilisation malveillante du DNS au niveau du GAC, ce qui nous a permis de mieux comprendre les différents cas d'utilisation malveillante des DNS du point de vue du GAC, y compris les démarches de collaboration dans le système, dans l'écosystème.

Aujourd'hui, nous allons passer en revue les preuves, nous allons partager les résultats de ce sondage du GAC et nous allons également avoir une présentation sur la conformité. Nous allons parler du rapport INFERMAL, nous allons parler du domaine Metrica et nous allons parler des étapes suivantes. Sur la base de la

discussion d'aujourd'hui, nous allons réfléchir à la suite et voir quelles sont les idées dont on pourra parler à Prague, en coopération avec tout l'écosystème. Ensuite, Martina, je vous cède la parole pour la suite.

NICOLAS CABALLERO Merci beaucoup, Tomo, et je suis ravie d'être avec vous et de présenter cette séance, même si c'est à distance. Je m'appelle Martina Barbero de la Commission européenne et je travaille sur ces questions d'utilisation malveillante du DNS avec Tomo. A partir de maintenant, je vais me concentrer sur la présentation des résultats du sondage du GAC sur l'utilisation malveillante du DNS. Nous avons effectué ceci au début de 2025. Nous allons passer à la diapositive suivante.

Donc voilà, c'est un sondage qui a été organisé conformément aux objectifs stratégiques du GAC et au numéro trois sur l'utilisation malveillante du DNS, avec pour objectif de mieux comprendre, du point de vue des membres du GAC, quelles sont les attentes et les préoccupations du gouvernement sur ce sujet et en tant que responsable de thématique, de voir comment nous pouvons, grâce aux séances ICANN en personne et intersession, comment répondre aux attentes des membres du GAC.

Nous avons donc lancé ce sondage en janvier. Nous l'avons terminé en février et nous avons reçu 21 réponses. Vous voyez sur la diapositive la distribution géographique. Donc, tous les continents sont représentés avec différents niveaux de participation, bien sûr.

Alors je fais une pause maintenant pour remercier sincèrement tous les membres du GAC qui ont envoyé leurs réponses à ce sondage, parce que c'était très utile pour nous de pouvoir rassembler ces perspectives. Même si nous n'avons pas d'échantillon représentatif, je crois que ceci nous informe dans le cadre de la planification de notre travail sur l'utilisation malveillante du DNS. Nous pouvons mieux voir quel est l'intérêt des membres du GAC par rapport à ces sujets d'utilisation malveillante du DNS.

Donc ensuite, avant de rentrer dans le détail, ce que nous souhaitions faire très brièvement, c'est de mentionner les grandes lignes qui ressortent de ce sondage, il y en a trois. Vous vous attendez peut-être à ça. Donc le sondage confirme que l'utilisation malveillante de DNS est une priorité pour les membres du GAC. C'est évident. Ce qui émerge également de ce sondage, c'est que les membres du GAC ont des démarches très divergentes sur ce sujet et des meilleures pratiques assez différentes ainsi que des définitions différentes. Donc il y a une certaine diversité par rapport à la gestion de l'utilisation malveillante des DNS par les membres du GAC, ce qui veut dire que ceci est d'autant plus intéressant.

Ce qui est également ressorti du sondage, donc deuxième point. Globalement, les membres du GAC apprécient les efforts qui sont mis en place pour lutter contre l'utilisation malveillante du DNS dans le cadre de la communauté de l'ICANN et dans le cadre d'ICANN.org. Mais il y a aussi la reconnaissance selon laquelle c'est un sujet extrêmement important et urgent et donc il faut en faire

plus. Il faut accélérer notre travail. Et dernier point par rapport à ce sondage, les membres du GAC ont la conviction que le GAC a un rôle important à jouer dans le cadre de la communauté de l'ICANN pour faire avancer le travail sur l'utilisation malveillante du DNS.

Et nous allons entrer dans le détail dans quelques instants. Mais sachez qu'il y a un certain nombre de choses que le GAC peut faire, y compris surveiller la conformité aux amendements des contrats et puis parler des élaborations de politique. On pourrait également produire des directives pour encourager la collaboration au sein de l'ICANN et en dehors de l'ICANN et également gérer les nouvelles tendances et partager les meilleures pratiques. Donc voilà les grandes lignes. Et s'il n'y a qu'une chose à retenir dans tout ça, je pense que c'est peut-être ça.

Rentrons maintenant dans le détail des différentes parties de notre sondage. Première partie. Mieux comprendre quelle est la définition de l'utilisation malveillante du DNS par les membres du GAC et quelles sont les meilleures pratiques qu'ils ont par rapport à cela et comment est-ce qu'ils sont en lien avec la communauté dans le cadre d'une coopération? La définition de l'utilisation malveillante du DNS adoptée par les membres du GAC est globalement celle de l'ICANN, puisque à 44 %, ils utilisent la même définition. Il y en a quelques-uns qui ont une définition plus large puisqu'ils couvrent également tout ce qui est nocif en ligne, tout ce qui est pédopornographie. Il y a quelques personnes qui travaillent

actuellement sur une définition, mais qui n'ont pas encore adopté de définition.

Comme je l'ai déjà dit dans les grandes lignes, ce qu'on a également vu dans les réponses, c'est que les membres du GAC avaient avait différentes démarches pour gérer l'utilisation malveillante des DNS. Les initiatives législatives, les cadres de politiques, les initiatives cyber avec les CERTs, et la collaboration avec les ccTLD, la collaboration avec d'autres acteurs au-delà de la communauté stricte du DNS de l'ICANN. Donc, il y a différents outils. Ce qui veut dire qu'il y a aussi différentes meilleures pratiques.

Parmi les meilleures pratiques, il y a dans les réponses les mesures proactives pour gérer l'utilisation malveillante du DNS, Les partenariats public privé, que ce soit avec les parties contractantes comme les bureaux d'enregistrement les opérateurs de registre ou d'autres partenaires, par exemple, de la société civile. Et puis, bien sûr, nous avons travaillé à faire adopter des normes de sécurité, y compris l'utilisation d'incitations financières, les initiatives, connaître son client. Et puis, chose intéressante, l'IA. On sait qu'il y a des dangers de l'IA, donc usurpation d'identité, les enjeux en matière d'utilisation malveillante du DNS, mais selon le sondage, les membres du GAC utilisent l'IA pour réagir et atténuer l'abus du DNS.

Et, puis, collaboration communautaire. Encore une fois, beaucoup d'acteurs qui sont impliqués dans le cadre de la collaboration avec

les membres du GAC depuis les fournisseurs de services Internet, les forces d'application de la loi, les CERTs, les autorités de la propriété intellectuelle, etc. Nous avons 60 % des membres qui ont répondu au sondage et qui nous ont dit qu'ils sont impliqués dans une collaboration qui a été mentionnée.

Deuxième partie du sondage. Donc, comment est-ce que les membres du GAC surveillent l'utilisation malveillante de DNS? Nous avons donc posé des questions sur les sources où est-ce qu'on trouve les données relatives à l'utilisation malveillante du DNS? Donc, il y a certaines tendances qui se dégagent dans le cadre des réponses. Il y a certains membres qui ont des sites consacrés qui publient des rapports sur la fraude. La plupart des GAC utilisent des sources externes et ils sont également impliqués dans le partage d'informations entre agences gouvernementales.

Beaucoup d'entre eux travaillent avec les CERTs. Et puis, il y a beaucoup de membres du GAC qui utilisent les sources provenant de l'ICANN, que ce soit les publications, les rapports, l'INFERMAL dont on va parler tout à l'heure, d'autres types de sources qui nous viennent de la communauté de l'ICANN et donc différentes démarches pour recueillir les données. Mais, c'est vrai qu'il y a quelques sources de données communes que nous avons pu dégager. Ça a été important de le savoir pour voir également quel est le type d'éléments de preuve dont on dispose lorsqu'on parle d'utilisation malveillante du DNS. Transparent suivant, s'il vous plaît.

Alors, un élément important de cette enquête visait en fait à comprendre le taux de satisfaction des membres du GAC et puis leur évaluation des efforts menés par la communauté de l'ICANN pour relever le défi, le défi des utilisations malveillantes du DNS et pour les atténuer. Alors, nous avons posé quatre questions qui ciblaient chaque fois des parties prenantes différentes. Une question notamment sur l'évaluation des efforts par les membres du GAC de l'organisation de l'ICANN.

Nous leur avons demandé également d'évaluer les efforts des bureaux d'enregistrement et des opérateurs de registre. Est-ce qu'ils sont efficaces par rapport à l'application de leur obligation contractuelle. Nous avons demandé aux membres du GAC également d'évaluer les efforts des Parties contractantes. Et, comme vous le voyez sur cet écran et je ne vais pas rentrer dans le détail, mais il existe quand même une certaine cohérence dans les résultats et dans les notations. On est peut-être un tout petit peu moins satisfait au sein du GAC vis à vis des efforts des parties contractantes. J'y reviendrai, mais dans l'ensemble, les membres du GAC apprécient les efforts menés par la communauté en ce sens et reconnaissent que ces efforts ont vraiment de la valeur. Transparence suivant.

Alors, rentrons un tout petit peu dans les spécificités concernant l'évaluation des membres du GAC par rapport aux efforts de l'ICANN pour atténuer les utilisations malveillantes du DNS. En général, les membres du GAC sont satisfaits des efforts, mais ils reconnaissent également que les progrès ne sont pas aussi rapides

qu'ils pourraient l'être et que l'efficacité pourrait être plus élevée également. Les membres du GAC encouragent l'organisation de l'ICANN et les autres parties à être beaucoup plus ambitieux au moment de se donner des objectifs dans ce domaine. Alors, concernant les efforts des parties contractantes, et bien je crois que généralement, en fait, les membres du GAC sont satisfaits et reconnaissent que des efforts sont effectivement réalisés et qu'ils sont considérables.

Mais, il existe encore beaucoup d'incohérences entre les parties contractantes. Certaines parties contractantes, en fait, ne font que le minimum, alors que d'autres sont beaucoup plus efficaces dans la lutte contre les utilisations malveillantes du DNS. Et, donc, effectivement, il faudra améliorer la donne si nous voulons améliorer la situation dans tout le secteur. Et, puis, par rapport au contrat avec le registre et les accords ou les contrats d'accréditation des bureaux d'enregistrement. Alors, là, au niveau des dispositions, les membres du GAC considèrent qu'une avancée a été réalisée, mais nous ne disposons pas de suffisamment de données pour mesurer l'efficacité de ces dispositions.

Et, puis, par rapport à la position du GAC sur cette question, les membres du GAC reconnaissent que certains domaines ne sont pas couverts par les amendements contractuels, qu'il y a encore des lacunes. Les amendements n'obligent pas, par exemple, les parties contractantes à adopter des mesures proactives et à signaler de manière plus transparente les efforts qu'elle mène. Et, puis, la couverture de toute la chaîne de valeur. Par exemple, les

revendeurs ne sont pas couverts. Certains membres du GAC lit cette question et la question de l'exactitude et ce sont des aspects qui ne sont pas encore couverts par les amendements contractuels. Et, ce sont des aspects que les membres du GAC considèrent comme étant importants, transparents, suivants.

Alors, je crois que c'est mon dernier transparent transparents sur cette enquête. La dernière partie de l'enquête portait sur les priorités pour les membres du GAC. Quelles devraient être les priorités? Justement, quand nous parlons d'utilisation malveillante du DNS. Quelles sont les priorités? Sur quoi devons-nous travailler, surtout pour préparer le prochain cycle de l'année prochaine pour les nouveaux gTLD? Alors, nous pouvons réunir en fait les réponses et les catégoriser en quatre grappes. Alors, le GAC, en fait, a un rôle à jouer pour suivre et surveiller la mise en œuvre des amendements, faire un travail de liaison en matière de conformité et puis faire en sorte que les normes sont plus élevées en matière de lutte contre l'utilisation malveillante du DNS avant le lancement du prochain cycle.

Et puis, effectivement, nous devons envisager peut-être des objectifs en matière d'élaboration de politiques. On en a parlé avec l'ALAC plus tôt. Il y a en fait plusieurs domaines qui devraient faire l'objet de PDP, notamment les modalités spécifiques d'utilisation malveillante du DNS. On pourrait se fonder également sur les conclusions du rapport INFERMAL pour adopter des mesures

proactives sur certains sujets qui peuvent être pertinents au moment de penser à des processus d'élaboration de politiques.

Il y a encore un autre groupe de réponses qui ont trait au rôle du GAC dans l'élaboration de directives et pour la promotion de la collaboration. Alors, quand je parle de promotion de la collaboration, je ne parle pas seulement du fait qu'il faut s'assurer que le GAC soit en dialogue avec les autres communautés au sein de l'ICANN. Il s'agit d'établir des liens avec les parties externes à l'ICANN. Certains membres du GAC ont le sentiment qu'il est important également de souligner le besoin d'élaborer des directives sur comment s'attaquer aux utilisations malveillantes du DNS de manière efficace, et ce, avant le lancement du prochain cycle.

Et, enfin, par exemple, nous avons eu des discussions en ce sens avec le SSAC hier. Le GAC en fait doit également et bien traiter de nouvelles tendances et partager les meilleures pratiques. L'évolution des technologies ne s'arrête jamais. Nous devons donc dégager les nouvelles menaces qui peuvent surgir face à ces évolutions par rapport à l'informatique quantique. Par exemple, le vol d'identité, tout ce qui a trait à l'intelligence artificielle. Et, il s'agit également d'habileté. En fait, le partage de bonnes pratiques et de meilleures pratiques, notamment entre les gTLD et les ccTLD, ça, c'est vraiment quelques-unes des idées soulignées par ou mises en exergue par les membres du GAC.

Et, un dernier point qui est revenu dans pas mal de réponses, mais qui n'apparaît pas ici, et bien c'est le lien entre les utilisations malveillantes du DNS et par exemple, les travaux sur les données d'enregistrement, notamment l'exactitude. Ce sont des éléments qu'il faut prendre en considération à l'avenir. Mais, je crois que ce transparent, en fait, est en train vraiment de nous donner une idée de nos travaux futurs en tant que responsable thématique au sein du GAC et ce sont en fait des points que nous devrions traiter lorsque nous parlons d'utilisation malveillante du DNS. Je crois qu'à ce stade, nous avons prévu peut-être une petite séance de questions-réponses pour voir si les participants n'ont pas de questions, Mais je vous repasse la Parole. Nico.

NICOLAS CABALLERO Merci beaucoup, Commission Européenne. C'est un plaisir d'écouter vos présentations. Avant de donner la parole à Tomo du Japon à ma droite, je vous passe la parole. Mesdames et Messieurs. Est-ce que vous avez des questions, des commentaires en salle ou en ligne? À vous la parole.

MARTINA BARBERO Je crois qu'il y a une question, une question sur l'échelle que j'ai montré dans l'un de mes transparents. Est-ce que ça va du meilleur résultat au pire résultat? Non, en fait, la note un, c'est le manque de satisfaction. La note quatre, c'est pleine satisfaction. Voilà,

l'échelle que nous avons suivie. En fait, c'est une échelle ascendante.

NICOLAS CABALLERO Merci Martina. Mesdames et Messieurs, commentaires, observations, questions, réflexions? Je ne vois pas de mains levées. Tomo Je vous repasse la parole.

TOMONORI MIYAMOTO Merci beaucoup. Alors, transparent Suivant. Merci beaucoup. Alors, maintenant, nous allons parler de la conformité et je vais maintenant passer la parole à Leticia de l'unité de conformité de l'ICANN. Leticia.

LETICIA CASTILLO Merci beaucoup. Je m'appelle Leticia Castillo, je suis directrice principale au sein de la conformité contractuelle de l'ICANN. Merci de me donner la possibilité de vous offrir une petite mise à jour concernant les exigences en matière d'utilisation malveillante du DNS.

J'ai reçu quelques questions à l'avance et j'ai essayé de les incorporer dans ma présentation aujourd'hui. Mais, bien sûr, si je n'ai pas tout couvert, je répondrai à vos questions très certainement par la suite. Transparent suivant. Transparent suivant. Désolé. Merci beaucoup.

Du 5 avril 2024 au 5 décembre 2024 au sein de la conformité, nous avons résolu 280 enquêtes pour ce qui a trait aux utilisations malveillantes du DNS à travers un mécanisme de résolution informel. Donc, il n'y a pas eu d'avis d'infraction formel qui a été requis, ce qui a abouti à la suspension de 2900 nom de domaine malveillant et la désactivation de 365 sites d'hameçonnage à la date du 5 mars 2025. Donc, la semaine dernière, et bien, nous avions 46 enquêtes d'atténuation d'utilisation malveillante du DNS en cours qui avaient déjà abouti à la suspension de 5400 noms de domaine malveillants. Donc, jusqu'à présent, donc, nos affaires ou nos cas en matière de conformité, et bien ont abouti à l'atténuation de 8000 cas d'utilisation malveillante des DNS.

Alors, cela est lié évidemment au plan de remédiation que nous avons lancé et que nous exigeons aussi de la part de nos membres pour qu'ils restent conformes. Et, tout cela est lié également aux actions prises par les bureaux d'enregistrement et les registres pour justement rester conformes aux obligations sans que l'ICANN n'est à les contacter. Nous avons envoyé trois avis d'infraction formelle en lien avec les exigences en matière d'utilisation malveillance du DNS. Ces avis sont délivrés uniquement lorsque nous avons épuisé notre processus informel sans trouver de solution. Alors, les processus informels impliquent une notification, un contact avec les parties. Nous offrons des informations également. Nous demandons des éléments de preuve concernant la conformité.

Mais, le processus peut être accéléré. Par exemple, lorsque nous découvrons qu'il y a des manquements répétés et qu'il y a effectivement des mesures correctives qui ne sont pas prises. Les trois avis d'infraction sont en cours et les parties contractantes sont en train de travailler sur les plans de correctifs qu'elles vont mettre en œuvre pour se mettre en conformité, pour rester en conformité à l'avenir. Et, nous continuons à surveiller la situation de ces trois parties contractantes. Alors, les extensions des dates limites sont peu courantes. En effet, lorsque les parties contractantes mettent en place des plans correctifs cela met du temps, mais nous n'accordons pas d'extensions comme cela.

C'est à dire que si des domaines malveillants continuent d'être actifs. Et, bien, là, nous ne prolongeons pas effectivement des extensions, surtout si ces sites malveillants causent des préjudices.

Alors, j'ai dit que nous avions 46 enquêtes en cours. 48 % plus ou moins de ces enquêtes ont été le résultat de plaintes déposées par des chercheurs en matière de sécurité de l'information auto identifiés. Nous avons des plaintes qui sont déposées par les juristes de propriété intellectuelle ou encore les associations de protection des marques. 13 % de nos plaintes proviennent de personnes qui s'identifient comme appartenant à d'autres groupes, par exemple des représentants d'entreprises victimes de vol d'identité, d'entreprises ayant reçu par exemple des courriels d'hameçonnage, etc. 24 % des cas et bien ont trait à, par exemple,

d'autres parties contractantes, des titulaires de noms de domaine, etc. Transparent suivant.

Alors, pour ce qui a trait à la distribution géographique des cas que nous traitons, la plupart des plaintes déposées proviennent de la région Asie, Australie et Pacifique, puis l'Amérique du Nord, ensuite vient l'Europe. Ensuite, vient l'Amérique latine et les Caraïbes.

Comme vous le voyez sur ce transparent, outre l'application de toutes les exigences contractuelles dans le processus de plainte. Nous menons deux cycles d'audit par an. Chacun dure à peu près six mois. Une équipe d'audit au sein de la conformité avec l'aide de KPMG évalue en fait les données recueillies auprès des parties contractantes et sur les parties contractantes pour évaluer leur conformité. Et, il faut également dire que les audits peuvent également aboutir à des avis d'infraction formelle et nous publions un rapport qui inclut nos constatations principales à la fin de chaque cycle.

En octobre, nous avons lancé un audit qui, en fait, comprend les contrats de registre. Il s'agit de confirmer et de vérifier que les opérateurs de registre comprennent bien leurs obligations et disposent des processus nécessaires pour être conformes à nos exigences. Alors, la sélection des entités contrôlées s'est fondée en partie sur des classements en interne et en externe en matière d'utilisation malveillante des DNS. Alors, le fait d'avoir été choisi ne veut pas dire que le TLD n'est pas conforme. Nous sommes en train de revoir toutes les informations, tous les enregistrements que

nous avons recueillis pour prendre une décision et nous allons publier un rapport avec nos constatations une fois que l'audit sera terminé.

Sur cette dernière diapositive, nous avons un résumé des différentes initiatives sur lesquelles nous travaillons. Nous devrions publier un rapport sur un an qui correspond à celui qu'on a publié sur les six mois, en incorporant certains des feedbacks qu'on a reçu de la communauté sur le rapport avec davantage d'informations sur le traitement des plaintes, le résultat des audits des supports éducatifs. Donc, tout ceci est en cours. Et, puis, les mises en vigueur. Récemment, nous avons rassemblé différentes informations par rapport aux campagnes d'hameçonnage et autres.

Donc, d'autres efforts, d'autres supports éducatifs. Nous sommes engagés au maintien de ces exigences et aux rapports de nos progrès. Je m'arrête là pour écouter les questions.

NICOLAS CABALLERO

Merci beaucoup Leticia. C'est fantastique cette présentation. Elle est très détaillée. Donc, faisons une pause maintenant pour voir s'il y a des questions ou des commentaires de la salle ou alors en ligne également. Je ne vois pas de mains en ligne et je ne vois pas de main non plus levée dans la salle. L'Inde allez-y, Essayez de parler lentement parce que je sais que vous avez tendance à... Donc, pour les interprètes, s'il vous plaît, parlez lentement.

PERSONNE NON IDENTIFIÉE Merci, Monsieur le président. Étant donné que le rapport explique que les récidivistes sont des bureaux d'enregistrement précis. Je ne sais pas si c'est pourquoi... Quelle est la raison? Est-ce que c'est une question d'enregistrement groupé ou un modèle de prix? Est-ce qu'il pourrait y avoir un processus de réflexion pour élaborer une notation de risque peut-être sur les bureaux d'enregistrement? Un mécanisme, ce qui qui nous indique un petit peu ceux qui ont un bon comportement, ceux qui n'ont pas un bon comportement.

LETICIA CASTILLO Merci. Je voudrais savoir si vous faites référence au diagramme que j'ai présenté? Ou est-ce que vous parlez de manière plus globale?

PERSONNE NON IDENTIFIÉE En général, ce n'est pas spécifique à votre présentation. Ma question, c'est ces audits, ce rapport INFERMAL nous montre que certains bureaux d'enregistrement par rapport aux mesures d'atténuation du DNS ne se comporte pas bien. Est-ce que c'est juste?

LETICIA CASTILLO L'audit est toujours en cours.

PERSONNE NON IDENTIFIÉE Mais, selon le rapport INFERMAL, beaucoup de récidivistes en matière d'utilisation malveillante de DNS ciblent en fait certains

bureaux d'enregistrement. En tout cas, c'est ça la constatation du rapport INFERMAL. Donc, l'idée c'est est-ce qu'il serait bon d'avoir une sorte de moyen d'évaluation pour voir un petit peu quelle est la performance des bureaux d'enregistrement en matière d'atténuation d'utilisation malveillante du DNS? Une sorte de début de notation.

LETICIA CASTILLO Je ne sais pas si je suis la bonne personne pour répondre à cette question, mais du point de vue de la conformité, nous avons un rôle limité pour donc faire appliquer les amendements aux accords, mais au sein de la conformité nous collectons beaucoup de données et nous revoyons toutes ces données. Je vous l'ai dit, nous faisons partie de cette initiative sur laquelle nous travaillons, donc qui est une initiative proactive de surveillance, et donc tout ce qui est échecs répétés, tendances générales, par exemple, ceux qui vraiment échouent plus souvent. Tout ceci, nous le prenons en compte dans la conception de ces actions de mise en vigueur proactive et dans le cadre de notre processus, nous prenons ceci en compte. Mais, je ne sais pas si je peux répondre directement à votre question.

NICOLAS CABALLERO Merci à l'Inde. Merci Leticia, Monsieur Andrews.

GABRIEL ANDREWS

Merci beaucoup Leticia pour votre présentation. J'aimerais bien savoir, vous parlez de la quantité de données que vous utilisez pour vos enquêtes. Vous en avez 46 je crois à ce jour, cette année, c'est déjà beaucoup et j'aimerais bien savoir quel est le type de données que vous avez tendance à demander des bureaux d'enregistrement. J'aimerais bien savoir si ces données impliquent les données relatives aux données d'enregistrement, aux titulaires de noms de domaine, aux détenteurs de comptes.

LETICIA CASTILLO

Lorsqu'on lance une enquête de conformité, on cible ceci selon les obligations qui sont relatives à la plainte en elle-même. Donc, on inclut des questions relatives aux données. En ce qui concerne les obligations en matière d'utilisation malveillante du DNS. Encore une fois, cela dépend de la plainte spécifique, mais globalement, nous fournissons une copie de la plainte et une copie des preuves et les autres points que nous considérons comme pertinents. Et, nous demandons une réponse détaillée de ce qu'a fait la partie contractante, quels ont été les actions mises en œuvre pour atténuer ou pour interrompre? Quelles actions ont été effectuées et s'il n'y a pas eu d'action et bien pourquoi? Nous demandons pourquoi et nous demandons ensuite des enregistrements.

Parfois, il y a différentes étapes qui sont entreprises et il y en a qui vérifient les comptes dans le cadre de la révision. Ils nous expliquent tout ceci, mais ce qui est demandé est vraiment ciblé par rapport à l'enquête, précise.

NICOLAS CABALLERO Merci. J'ai la République dominicaine ensuite.

PERSONNE NON IDENTIFIÉE Merci président. Je vais parler en espagnol si vous le permettez. Leticia, je ferai une toute petite observation, puis je poserai une question. Alors, c'est vrai que je suis plus tranquille parce que lors de la séance précédente, on a traité de cette question de l'utilisation malveillante du DNS et on avait l'impression que les choses sont un petit peu en suspens, mais maintenant je me rends compte que, en fait, il y a vraiment un travail et un travail effectif qui est mené. Je vois les chiffres, comme le disait l'orateur précédent, c'est vrai que les chiffres sont assez impressionnants pour ce qui a trait aux exigences, pour ce qui a trait à vos enquêtes. Voilà, qui nous tranquillise beaucoup en tant que gouvernement et en tant que pays.

Alors, ma question, ces rapports, ces audits, ces rapports d'audit sont-ils publiés en ligne? Peut-on les lire et les consulter? Parce que pour nous, dans nos stratégies de cybersécurité et tout autre domaine que nous suivons notamment et bien justement, la pédopornographie notamment, ou alors l'exploitation des enfants, des femmes, la violence envers les femmes, et bien ces rapports d'audit peuvent être vraiment des éléments qui peuvent nous permettre de mieux comprendre la situation et de dégager les tendances. Merci.

LETICIA CASTILLO

Merci. Merci beaucoup! Je vais répondre en espagnol. Et, bien, merci! Merci beaucoup pour cette question. Alors, c'est vrai que nous saisissons beaucoup de données, d'informations concernant les cas qui nous sont soumis, que nous traitons et nous avons des rapports, des rapports que nous publions mensuellement et qui comprennent notamment bien sûr tout ce qui a trait aux obligations concernant l'utilisation malveillante des données, mais aussi toutes les obligations concernant les contrats de l'ICANN.

Pour les utilisations malveillantes du DNS, nous avons un rapport spécifique concernant les actions que nous entreprenons par rapport aux exigences. C'est un rapport mensuel qui reprend bon nombre de données et en fait, nous avons différents chapitres selon le type d'utilisation malveillante du DNS. Par ailleurs, nous publions un rapport peut-être plus fourni avec plus d'exemples, plus d'informations, de contexte. Parfois, le fait de n'avoir que des données, et bien ces données ne sont pas explicatives. Il faut vraiment donner un cas, un exemple pour que ça ait du sens.

Alors, ce dernier rapport a été publié sur notre site le 8 novembre dernier et nous sommes en train de travailler sur la publication d'un autre rapport avec plus d'informations, de contexte, plus d'exemples. Et, nous avons incorporé également le feedback, le retour de la communauté sur le précédent rapport. Justement concernant le respect des obligations et concernant les audits,

nous avons des rapports à part entière qui sont publiés à ce niveau. Merci beaucoup.

NICOLAS CABALLERO

Merci beaucoup Leticia, J'ai la Suisse et ensuite il faudra que je ferme la file d'attente pour la deuxième fois parce qu'il faudra continuer la présentation.

JORGE CANCIO

Merci Nico. Merci pour cette séance, en particulier à vous Leticia pour toutes ces informations. Je voulais simplement vous faire part de quelques perspectives par rapport à la discussion avec notre police fédérale en Suisse. Ils voient l'effet positif des amendements au contrat. Donc, ceci est bon signe. Il observe également, en même temps que certains bureaux d'enregistrement ne collaborent pas nécessairement comme ils le devraient. Et, donc, nous ne sommes pas certains de ce qu'il faudrait faire pour davantage les motiver. Ces bureaux d'enregistrement qui ne semblent pas collaborer et qui semblent agir comme ils l'entendent. Nous ne savons pas exactement ce que nous pourrions faire. On pourrait peut-être vous en faire part directement à la conformité, peut-être vous fournir ces données. Ça pourrait être un aspect important.

Nous avons également reçu comme retours qu'apparemment, les plaintes en matière d'abus des agences d'application de la loi ne sont pas toujours prises au niveau de sérieux qu'on pourrait

attendre. Donc, il y a des préoccupations à ce niveau là parce que la légitimité parfois est remise en question alors qu'il semblerait qu'il est très clair que les personnes qui les envoient sont absolument légitimes. Donc, voilà, je voulais vous faire part de ces informations.

LETICIA CASTILLO

Merci pour ce commentaire. Du point de vue de la conformité, je vais essayer de me rappeler de tout ce que je voulais dire, mais nous les encourageons à nous envoyer une plainte. Nous avons un formulaire web. Tout ceci est public. Nous recevons des milliers de plaintes par an par ce moyen. Nous avons plusieurs questions dans le formulaire qui ont pour objectif de rassembler les informations. Si la plainte est reçue par les forces d'application de la loi, ceci est repéré par notre système. Donc, nous savons quel est le type. Tout ceci est surveillé par le système. Donc, nous encourageons tous ceux qui pensent qu'une partie contractante n'est pas fidèle à ses obligations à nous le dire.

Nous avons un système établi qui nous permet d'assurer la mise en vigueur lorsqu'un processus passe à une violation formelle. Nous avons s'il n'y a pas solution, donc une résiliation, une suspension d'abord et une résiliation ensuite pour le bureau d'enregistrement. En ce qui concerne les agences d'application de la loi, je les encourage à nous contacter. Il ne faudrait pas qu'ils se mettent à croire que nous ne prêtons pas attention à leurs plaintes. Nous sommes attentifs à toutes les plaintes. Je ne sais pas si peut-être ils

font référence aux plaintes qui sont envoyées, indiquant qu'ils sont une agence d'application de la loi dans la juridiction et dans la juridiction où se trouve le bureau d'enregistrement. Si ce n'est pas clair, quelle est la juridiction? Quelle est la compétence qui s'applique? Eh bien, cela ne veut pas dire qu'on ne va pas traiter la plainte. Nous allons la traiter, mais nous devons savoir si la compétence et le ressort s'appliquent à la partie de l'accord dont nous nous assurons la mise en vigueur. Je ne sais pas si c'est à ça que vous faites référence, mais je voulais le mentionner.

NICOLAS CABALLERO Merci Leticia, merci la Suisse. Je vais maintenant repasser la parole à Tomo pour la suite de la présentation. Tomo.

TOMONORI MIYAMOTO Merci beaucoup! Merci pour votre mise à jour sur la conformité. Je serais heureux de voir vos rapports futurs et vos travaux futurs. Ensuite, je vais demander au bureau de la technologie de l'ICANN avec Sion qui est avec nous, de faire sa présentation sur le rapport INFERMAL.

SIÔN LLOYD Merci beaucoup. Je m'appelle Sion Lloyd. Comme vous l'avez entendu, je travaille pour le bureau de la technologie à l'ICANN. Je vais vous présenter deux projets. D'abord domaine Metrica et INFERMAL, deux projets de l'ICANN.

Tout d'abord par rapport à Domaine Metrica. De quoi s'agit-il? Et, bien, il s'agit d'un système qui collecte les données sur les noms de domaine et qui ensuite rend ces données utilisables, téléchargeables pour différents utilisateurs et sous différents formats.

Nous avons les données au niveau du nom de domaine et nous pouvons ensuite cumuler tout ceci au niveau du gTLD, au niveau du bureau d'enregistrement. Ce sont des données dans lesquelles on peut faire des recherches. On peut avoir des métadonnées, on peut avoir du contexte sur la base des différentes entités, des différents domaines, des différents gTLD que l'on cherche. Nous avons également des données au niveau du domaine dans lesquelles on peut faire des… ou que l'on peut partager. Il y a différentes visualisations, différentes chat sur une interface web, il y a des API application de programmation d'interface. Donc, on peut utiliser des codes, des scripts éventuellement si cela est préférable. Ensuite.

Donc, je ne vais pas vous présenter toutes les fonctionnalités, mais quelques exemples rapides. Si par exemple, vous recevez un email ou un message texto sur un domaine que vous ne connaissez pas bien, vous pouvez donc l'informer. Vous allez recevoir des informations de contexte. Quel est le bureau d'enregistrement qui a parrainé la création, les différents et différents réglages?

Et, vous allez également voir si nous avons connaissance de certains signalements d'abus sur ce domaine et quel est le

fournisseur qui a signalé cet abus. Il y a aussi une ligne de tendance, donc un diagramme. Nous utilisons le classement Tranco et vous pouvez savoir quelle est la considération par rapport à ce nom de domaine.

Alors, on peut évidemment effectuer des recherches au niveau du TLD. Et là, encore une fois, vous avez accès à des informations de contexte, le registre, la taille du TLD, les changements nets depuis que nous l'avons mesuré et vous recevez des statistiques sur le volume d'utilisation malveillante, tant en tant que pourcentage de la zone dans sa totalité notamment.

Et, vous recevrez également d'autres informations, par exemple les tendances en matière d'utilisation signalée, malveillante, signalée une géolocalisation également des domaines en cause où nous pouvons alors voire où ces domaines sont hébergés. Transparence suivante.

Nous avons parlé de données de niveau de domaine qui sont partageables en tant qu'opérateur de registre ou en tant que bureaux d'enregistrement et utilisateurs du système. Vous avez accès à la liste de domaines que vous gérez dans votre TLD ou vous êtes peut-être le bureau d'enregistrement parrain de ce nom. Et, là, vous avez bien sûr des informations sur qui a signalé le domaine, le type d'utilisation malveillante. Par exemple, un réseau zombie, logiciels malveillants. Dans la plupart des cas, il s'agit d'hameçonnage.

Alors, Domain Metrica n'est pas un produit fini en soi. Pour l'instant, nous pensons qu'il va évoluer tout au long de son cycle de vie avec de nouvelles mesures, de nouvelles sources de données sur la base des recherches que nous aurons pu mener. C'est une plateforme véritablement qui nous permet d'approfondir nos recherches. Nous pouvons la faire évoluer sur la base du retour que nous recevrons de la communauté puisque c'est une plateforme qui est disponible à quiconque a un compte ICANN. Quiconque s'inscrit à une réunion de l'ICANN a accès aux données Domain Metrica. Là, je vous ai mis sur l'écran quelques liens vous renvoyant vers une petite page avec plus de détails et vous avez aussi une foire aux questions, d'autres documents auxquels vous aurez accès. Et, puis, il y a un lien vous renvoyant vers un webinaire où vous pourrez trouver d'autres informations sur les fonctionnalités notamment qu'offre Metrica. Transparence suivant.

Alors, je vais passer maintenant au projet INFERMAL et au rapport Infermal d'analyse impériale de domaine enregistré malveillant. Je crois qu'on en a déjà parlé de ce rapport.

Alors, il s'agit d'un projet qui a été financé par l'ICANN, mais les travaux ont été menés en soi par un groupe sous la direction du professeur Maciej Korczyński, de KOR Labs à l'Université de Grenoble et c'est un projet qui s'est penché sur les politiques en matière d'enregistrement, les pratiques également pour dégager les tendances qui font que les pirates préfèrent l'un ou l'autre, l'une ou l'autre combinaison TLD, bureau d'enregistrement. Ce rapport final a été publié à la fin de l'année dernière. Comme je le disais,

vous trouverez d'autres détails en suivant le lien que je vous ai mis à l'écran. Alors, il y a un lien qui vous renverra vers un rapport qui est très détaillé, je dois dire, très approfondi. Et, puis il y a un webinaire qui a été organisé sur la question plus tôt cette année. Transparent suivant.

Alors, INFERMAL, qu'a-t-il fait? Et, bien, INFERMAL s'est penché sur les différentes fonctionnalités caractéristiques d'un enregistrement. Par exemple, les prix. A t ont appliqué des remises, par exemple des remises, des rabais si l'on fait par exemple des enregistrements groupés ou de plusieurs noms en même temps. Alors, en parlant de l'enregistrement groupé, y a-t-il des facilités en ce sens? Alors, encore une fois, les API, les interfaces de programmes d'application. Alors, quelles sont les interactions qui sont possibles entre l'usager et le processus d'enregistrement? Quelles sont les méthodes de paiement qui sont disponibles? Peut-on parler en crypto monnaie avec PayPal? Et puis, quels sont les autres services disponibles dans le cadre ou offerts dans le cadre des frais d'enregistrement, par exemple l'hébergement web, un certificat TLS? Qu'est-ce qui est pris en charge pour vous dans le cadre de ce processus d'enregistrement? Tout cela, ce sont des paramètres sur lesquels l'étude s'est penchée.

D'autres caractéristiques sur lesquelles nous nous sommes penchés, c'était plutôt les pratiques de vérification et de sécurité. Certaines pratiques étaient proactives, par exemple la validation des coordonnées de contacts avant l'acceptation de paiement pour l'enregistrement. Quels types de restrictions sont en place?

Avez-vous besoin d'être présents localement dans le territoire où vous demandez l'enregistrement? Quels sont les documents requis et puis quelles sont les mesures proactives qui peuvent être prises, notamment pour empêcher des abus ou l'enregistrement de noms malveillants.

Par exemple, si j'ai une chaîne comme Office 365 ou Facebook, et bien là je suis plus susceptible d'être victime d'hameçonnage. Est-ce que cela est vérifié avant l'achat du domaine? Et puis, outre les mesures proactives, nous avons dans l'étude INFERMAL mesurer des mesures réactives, par exemple le temps de disponibilité. Alors, combien de temps les domaines signalés restent actifs avant qu'une mesure d'atténuation ne soit prise et appliquée?

Alors, divers ensembles de données ont été utilisés dans l'étude. Je ne vais pas tout passer en revue, mais en fait là, on a mélangé. Et, bien, les données de tiers par de tierces parties des données recueillies manuellement, c'est à dire en passant en revue ce qui était disponible tout au long du processus, et des mesures du DNS, des mesure WHOIS, etc. Des mesures actives?

Alors, le rapport en soi est extrêmement détaillé et il y a beaucoup de nuances. C'est à dire que l'on met tous ces chiffres en contexte. Alors, je ne peux vraiment pas tout résumer en cinq transparents, mais j'essaie de vous donner ici une idée de ce que vous verrez dans le rapport. Alors, il y a de très fortes corrélations avec une augmentation des utilisations malveillantes par rapport à une disponibilité d'API gratuite, de DNS ou d'hébergement gratuit. Et,

puis, la présence de remises au moment de l'enregistrement. Voilà, cela semble être lié avec une augmentation de l'utilisation malveillante. Par ailleurs, il y a diminution des utilisations malveillantes, apparemment en corrélation avec la validation, par exemple des courriels, des numéros de téléphone, c'est à dire des coordonnées de contact, et s'il y a aussi présence de restrictions au moment de l'enregistrement.

Et, l'auteur, en fait, lorsqu'il a présenté son travail, lui-même a voulu souligner certains éléments. Par exemple, il est possible que les pirates soient attirés par une série de facteurs. Il n'y a pas un seul facteur qui attire les pirates. Il est également important de tenir compte d'autres implications de décisions prises sur la base de ces données. Alors, une décision peut supposer ensuite que, par exemple, un utilisateur malveillant va choisir un autre bureau d'enregistrement ou un autre TLD, mais il y a peut-être d'autres éléments qui entrent en ligne de compte. Et, c'est vrai que les pirates vont répondre aux mesures qui sont mises en œuvre et modifier leur comportement.

Pour terminer, j'aimerais surtout remercier le professeur Korczyński et son équipe pour l'incroyable travail qui a été mené et pour ce rapport extrêmement détaillé qu'ils ont pu formuler. Voilà, je m'arrête là et si vous avez des questions, n'hésitez pas.

NICOLAS CABALLERO Merci beaucoup pour cette présentation très, très intéressante Monsieur Lloyd, surtout concernant un fait très simple, à savoir le

fait qu'il y a un courriel, donc une adresse de courrier électronique, un numéro de téléphone qui sont exigés et la validation de ces coordonnées semble être corrélée à une diminution des utilisations malveillantes du DNS. C'est très intéressant. Alors, il nous reste cinq petites minutes peut-être pour une mini session de questions réponses. Mesdames et Messieurs, à vous la parole en ligne ou en présence. Je vois qu'une main se lève au fond de la salle. Vous prenez l'un ou l'autre micro. Allez-y, posez votre question.

ALEX URBELIS

Alex Urbelis de nom de service Ethereum. Alors, on parlait de métriques et des statistiques que vous recueillez concernant justement aux menaces. Vous avez parlé de localisation de l'hébergeur. Alors, très souvent, mon expérience me montre qu'on se cache derrière des nuages informatiques. Alors, comment? … ou notamment sur Cloudflare? Alors, est-ce que vous demandez des informations de géolocalisation à Cloudflare? Ou comment recoupez-vous les informations exactement?

SIÔN LLOYD

Alors, c'est en fait une géolocalisation qui résulte en fait des adresses IP pour les domaines que nous étudions. Nous savons qu'il y aurait des inexactitudes, des incohérences dans ces données, mais ces données peuvent potentiellement montrer quelque chose d'inattendu ou d'intéressant pour les parties.

ALEX URBELIS Alors, est-ce que ces données sont actualisées en temps réel ou a posteriori?

SIÔN LLOYD Quotidiennement.

ALEX URBELIS Alors, nous pouvons signaler un domaine et l'ICANN va ouvrir une enquête et actualiser alors la Metrica au quotidien.

SIÔN LLOYD Non. Alors, nous utilisons la liste de réputation et de blocage à ce sujet.

NICOLAS CABALLERO Merci beaucoup. L'UPU. Tracy.

TRACY HACKSHAW Tracy Hackshaw de l'UPU. Concernant le site de Metrica, je venais de le vérifier. Je me demandais si effectivement on peut procéder à des comparaisons. Est-ce que l'on peut faire une analyse comparative, par exemple entre TLD? Est-ce que c'est une caractéristique ou une fonctionnalité que vous allez mettre en ligne?

SIÔN LLOYD Oui, vous pouvez le faire d'ailleurs, mais venez me voir après cette session, je peux vous montrer comment faire justement.

NICOLAS CABALLERO Merci à l'UPU. D'autres questions et observations avant que nous passions au point suivant? Alors, c'est encore une main levée, une ancienne main levée Tracy? Oui, merci beaucoup Tomo. Je vous repasse la parole. Désolé, je suis désolé. Le Cambodge.

PERSONNE NON IDENTIFIÉE Bonjour à tous! Le Cambodge au micro. Po du Cambodge. J'aurais une question. C'est peut-être une question au président du GAC, Nico. J'aimerais poser la question au GAC ou à l'ICANN. Y a-t-il des directives, l'une ou l'autre directive, l'un ou l'autre règlement, une ventilation des types d'utilisation malveillante du DNS? L'une ou l'autre décision concernant justement ces utilisations malveillantes du DNS. Ce matin, vous avez parlé d'une enquête en matière de conformité. On a parlé d'atténuation, mais je ne vois rien de contraignant, pas de règlement, pas de réglementation pour la protection face aux utilisations malveillantes du DNS.

NICOLAS CABALLERO Merci le Cambodge. Est-ce que vous pouvez répéter votre question? Je n'ai pas bien compris.

PERSONNE NON IDENTIFIÉE Oui. Ma question, c'est donc que le GAC et l'ICANN ont des réglementations, des directives pour la protection contre l'utilisation malveillante du DNS, contre les problèmes relatifs au DNS.

NICOLAS CABALLERO La réponse courte, c'est que non, le GAC n'a rien de spécifique. Il y a des recommandations qui viennent de l'ICANN, de l'Institut Net Beacon et d'autres instituts, et on peut certainement vous guider vers le bon endroit. Par exemple, mise en application du DNSSEC. Nous avons une excellente équipe au sein de l'ICANN qui peut absolument vous aider avec tout ça. Il n'y a pas que la mise en application du DNSSEC, mais il y a les RKPI et puis d'autres exemples, d'autres initiatives et mesures que vous pouvez mettre en œuvre dans vos pays, ce n'est pas un souci. Mais le GAC en lui-même n'a pas de directives spécifiques. Certes, ça ne serait pas une mauvaise idée d'avoir une sorte de package préparé. Merci au Cambodge pour la question. Sans plus attendre, je cède la parole à Tomo.

TOMONORI MIYAMOTO Merci beaucoup pour ces informations d'OCTO. Ensuite, nous allons passer au panel. Nous avons donc Graeme de NetBeacon. Nous avons Reg et Luc des bureaux d'enregistrement. Alors ces questions de la discussion d'aujourd'hui sont à poser au panel.

Quelles sont vos réactions par rapport aux données, aux informations de Domain Metrica et du rapport INFERMAL. Et quelles constatations est-ce que vous souhaitez souligner? Donc vous êtes là présents au panel. Vous allez pouvoir commencer par vos courtes remarques sur ces sujets et ensuite nous ouvrirons la discussion sur vos questions. Donc Graeme d'abord.

GRAEME BUNTON Oui. Bonjour. Merci. Je suis Graeme. Je suis directeur exécutif de l'Institut NetBeacon. Notre objectif est de sécuriser l'Internet en luttant contre les domaines malveillants. Donc j'ai quelques diapositives. Je vais les présenter rapidement pour ne pas perdre de temps parce que je sais que mes collègues ici souhaitent également avoir le temps d'intervenir.

Donc pour commencer, bravo au professeur Korczyński, à l'ICANN, à Samaneh et à toute l'équipe de technologie pour leur travail sur INFERMAL. C'est un excellent rapport, très intéressant. Il est important. J'ai peut-être un petit problème avec le rapport, c'est que c'est un travail que nous souhaitions faire, mais c'est eux qui y sont arrivés en premier. Donc voilà, c'est très bien. Ce qui est très bien dans ce rapport, c'est qu'il donne les grandes lignes de toutes les complexités de l'utilisation malveillante des DNS. Donc il y a 73 facteurs importants et fonctionnalités différentes qui sont un facteur. Si chacune de ces fonctionnalités pouvait être ajustée sous forme de manette, si celles-ci pouvaient donc être liées à ces

différentes fonctions, ce serait de cette manière qu'il faudrait penser au problème.

Je crois que INFERMAL nous a donné des données concrètes sur les questions qui, pour nous dans la communauté, étaient impliqués depuis longtemps dans l'utilisation malveillante du DNS. Et donc nous avons maintenant quelque chose sur quoi travailler pour nous donner des indicateurs de performance. Nous avons parlé de surprises. Eh bien moi, j'ai été surprise par le lien très bas entre la rapidité d'atténuation d'un bureau d'enregistrement et la rapidité ou le niveau d'abus. Moi, je pensais qu'il serait moins attrayant pour les mauvais acteurs s'ils étaient rapides et proactifs. Mais c'est quelque chose qui est intéressant dans le rapport parce que c'était peu présent.

Que devons-nous faire en tant que communauté? Je crois que beaucoup de personnes seraient intéressées par un PDP sur l'utilisation malveillante. Mais avant, je crois qu'il faut établir les principes. J'écoutais le sondage du GAC et la présentation qui a été faite et j'ai trouvé que c'était intéressant. Dans votre sondage, l'idée était d'avancer plus rapidement. Eh bien, comment le faire? D'abord, il faut identifier un problème spécifique qui, selon nous, pourrait donner lieu à des progrès importants rapidement. On ne peut pas lancer un PDP sur l'abus. C'est un sujet beaucoup trop large. Ça ne fonctionnera pas, ça prendra des années et on sera tous frustrés. Ce qu'il faut, c'est identifier un problème spécifique et commencer de manière très focalisée, de manière si focalisée que ce soit vraiment très étroit. Il faut presque que les gens soient

mal à l'aise, presque au niveau où les gens se diront : Mais de toute façon, le résultat, il est clair, mais je crois que c'est comme ça. Petit à petit, continuons de faire avancer le ballon sur le terrain graduellement pour pouvoir faire des progrès. Et puis je crois qu'il faut que ceci s'applique dans tout l'écosystème. Donc pas trop technologique, pas trop commercial.

D'autres points dans le cadre de ce travail, je crois qu'il faut se rappeler que les criminels sont plus rapides, plus intelligents. Très souvent, ils ont de meilleures ressources que nous et ils ne suivent pas les règles du jeu. Donc, on ne peut pas produire de politiques spécifiques. Certaines choses, comme par exemple limiter certains services parce que les mauvais acteurs vont s'adapter et il va nous falloir des années pour produire des politiques. Et nous savons que d'ores et déjà, ils font des automatisations contre les bureaux d'enregistrement qui ne proposent pas de services d'API.

Donc il nous faut des stratégies pour permettre au bureau d'enregistrement d'ajuster ces petites manettes dont je parlais – ces 73 fonctionnalités – dans leur contexte, qu'ils puissent mettre en place des frictions qui ont un impact sur les mauvais acteurs, mais pas sur les titulaires de noms de domaine qui sont innocents. Il faut que ceci soit applicable et qu'on puisse vérifier, auditer. Donc comment rendre ceci plus concret? Encore une fois, vous vous dites oui, cet accès API gratuit augmente le niveau d'abus. Et bien comment pousser les bureaux d'enregistrement à être plus prudents par rapport à ceux à qui ils permettent l'accès.

Et je crois que c'est là qu'on peut essayer de trouver des politiques qui puissent s'adapter au marché, qui puissent gérer non seulement l'abus actuel, mais l'abus futur. Alors plusieurs choses par rapport aux données et aux rapports d'abus, l'abus des bureaux d'enregistrement. Les rapports d'abus d'enregistrements, on en reçoit tous les jours. Nous avons un projet similaire à Metrica qui s'appelle MAP. On en est au tout début. Ce n'est pas conclusif, mais nous avons de plus en plus une augmentation des taux d'atténuation suite aux amendements au contrat. Donc, nous allons continuer de publier des contenus pour cette communauté. Nous allons continuer de vérifier ce qui se passe, mais nous encourageons cette communauté à réfléchir là-dessus.

Merci beaucoup. Reg.

TOMONORI MIYAMOTO

Merci beaucoup. Je suis donc au bureau d'enregistrement et je travaille avec Tucows. J'aimerais revenir sur un commentaire qui a été soulevé pendant la présentation. On a demandé à ce qu'il y ait un site web centralisé où les gens puissent envoyer des rapports. Eh bien, c'est exactement ce que Graeme nous propose. Net Beacon est un portail centralisé de signalement des abus de domaine et c'est accessible à tous. Pas besoin de se rendre vers le bureau d'enregistrement spécifique, je voulais donc le mentionner, parce que ça répond directement à la question qui a été posée.

REG LEVY Merci Reg.

TOMONORI MIYAMOTO Ensuite, Jeff.

JEFF BEDSER Merci. J'ai déjà parlé dans le contexte du SSAC avec le GAC en début de semaine, donc je veux simplement revenir sur certains des points. Je crois que l'étude INFERMAL est excellente. Je félicite les chercheurs et l'OCTO pour leur travail. Mais je l'ai déjà dit tout à l'heure, ce n'était pas un rapport sous forme de recommandation, c'était un rapport de constatation, ce qui confirme ce qu'on suspectait depuis déjà longtemps. Mais la confirmation, c'est la suivante : c'est une question économique. Les gens achètent les ressources les moins chères et les gens utilisent les ressources les plus simples pour y arriver, quelle que soit la motivation, criminelle ou non.

En termes de cybercriminalité, c'est des dizaines de milliards de dollars par an et donc la motivation pour les mauvais acteurs, qui est de subtiliser des services, leur motivation, c'est toujours le prix. Et donc ils vont chercher les services les moins chers. S'ils investissent 1 000 $ et qu'ils font des centaines de milliers de gains, des centaines de milliers de dollars, l'impact sur eux est ce qu'ils vont considérer.

Avec cette économie qui représente des dizaines de milliards et de milliards de dollars, il faut donc absolument mieux signaler. Il faut

mieux détecter. Nous sommes dans un domaine où les RBL sont utilisés pour mesurer le problème : 5 à 7, parfois 8 d'entre eux recherchent le haut de l'iceberg. Ce sont les données publiques auxquelles tout le monde a accès.

Tous les bureaux d'enregistrement, tous les opérateurs de registre ont des centaines de milliers de rapports tous les ans. Et ces rapports n'arrivent jamais sur ces listes et ils agissent là-dessus. Et donc la réalité, c'est que tout le monde dans cette salle, et si vous n'êtes pas d'accord, dites-le-moi, mais tout le monde a reçu un hameçonnage et l'a effacé et ne l'a pas signalé. C'est peut-être déjà arrivé cinq fois depuis le début de la journée. Le signalement est insignifiant. On sait que le problème est énorme, mais on ne sait pas exactement quelle est l'énormité du problème. Et donc il faut absolument travailler en tant que communauté, détecter le plus rapidement pour atténuer le plus rapidement possible. Nous devons donc travailler sur des technologies dans la communauté pour vous permettre de mesurer les preuves. Et je crois que dans le cadre des obligations contractuelles, c'est ça. Il faut qu'il y ait un rapport sur les preuves.

Les parties contractantes, les ccTLD, sur un rapport avec des preuves, peuvent travailler plus rapidement. Ils n'ont pas besoin de refaire l'enquête, ils peuvent rapidement utiliser ce qu'il y a et ensuite atténuer. Donc je pense que c'est dans ce sens qu'il faut avancer le rapport INFERMAL a vraiment clarifié les choses dans une réalité économique. La cyber économie, la cybercriminalité dans cette économie est d'ampleur et donc il faudra trouver des

solutions pour mieux signaler et pour mieux détecter les abus. Merci.

TOMONORI MIYAMOTO

Merci beaucoup pour vos observations. Bien, Mesdames et Messieurs, maintenant nous commençons notre séance de questions-réponses. Vous avez des questions ou des observations? Reg?

REG LEVY

Reg Levy pour le groupe de représentants des bureaux d'enregistrement. J'aimerais également souligner le bon travail que fait Jeff et son équipe. Alors c'est vrai que CleanDNS travaille en étroite collaboration avec Net Beacon. Et puis le délégué, un des délégués, a posé une question sur les modèles d'IA qui nous permettraient de lutter contre les utilisations malveillantes. Alors nous nous rendons compte en fait que l'IA est utilisée pour créer plus de méthodes d'utilisation malveillantes, mais ce sont des outils LLM notamment. Et Jeff justement, dans son entreprise, a tout un arsenal d'outils LLM qui nous permet d'agir beaucoup plus rapidement. Voilà.

NICOLAS CABALLERO

Merci Reg. N'hésitez pas à prendre la parole, prenez un micro et posez votre question. Allez-y, monsieur.

DEAN MARKS

Merci. Dean Marks, unité constitutive Propriété intellectuelle. J'aurais une question à l'adresse de Jeff concernant le fait que vous avez souligné le fait qu'il faut signaler et détecter les abus. Alors, par rapport au travail que vous menez, alors il me semble que c'est plutôt une position réactive. Que pensez-vous de mesures que l'on pourrait prendre à titre préventif pour éviter les utilisations malveillantes du DNS? Vous avez parlé de prix. Peu importe si vous avez en fait un prix minimal de 1 000 $, les cybercriminels continueraient à acheter des noms de domaine. Donc, apparemment, le prix n'a pas d'importance. Quelles pourraient être les mesures de prévention, notamment des mesures de Know your customer, c'est-à-dire Connaître son client? Est-ce que ce serait une mesure préventive?

JEFF BEDSER

Merci beaucoup, Dean, pour une excellente question. Alors historiquement parlant, les processus Know your customer – Connaître son client – avec des validations, des coordonnées par exemple sont de bonnes mesures. J'ai fait une présentation cette semaine d'ailleurs où je disais qu'il y a maintenant la présence de l'IA qui permet notamment potentiellement de créer d'autres identités en utilisant par exemple un nom de personne avec la photo d'une autre personne, notamment l'usurpation d'identité. Et bien tout cela est là. Ces menaces sont là et vous voyez que si l'on met des exigences de validation de données, vous verrez bien sûr des fraudes y associées qui vont croître.

Vous avez aussi des cybercriminels qui veulent en fait acheter un domaine avec une certaine extension parce qu'ils sont convaincus que cela va leur permettre d'accroître les possibilités d'escroquerie, ils le feront.

Je crois que la clé ici, ce sera… Et j'ai déjà vu que des initiatives étaient prises au niveau des opérateurs de registre et des bureaux d'enregistrement en ce sens. Eh bien, je crois que la solution passera par la collaboration. Chacun de ces acteurs doit traiter des centaines de milliers de signalements par an. Et alors effectivement, on peut essayer de relier ces rapports pour détecter des tendances qui nous permettraient de détecter d'autres cas. Alors par exemple, si Tucows par exemple identifie un cas de malveillance, d'utilisation malveillante et que là en fait on désactive un site notamment, on pourrait peut-être essayer de partager ces informations pour désactiver d'autres domaines.

Et je crois que ce sont des choses qui peuvent se produire s'il y a collaboration. Les domaines ont une date d'expiration par exemple. Alors c'est vrai que par exemple, l'infrastructure sous-jacente, par contre, est beaucoup plus pérenne. Et puis il y a une question de réputation à maintenir. Donc c'est là qu'il faut investir les efforts. Alors, les processus de paiement. Vous voyez, si vous avez de l'hameçonnage via des cartes de crédit, bon, il ne s'agit pas uniquement de désactiver ou de fermer les sites ou les domaines utilisés. Il faut pouvoir s'attaquer également au processus de paiement. Parce que bien sûr, les cybercriminels peuvent bien sûr

travailler sur le domaine. Mais si on s'attaque sur le flux d'argent, les flux de fonds, c'est encore plus intéressant.

NICOLAS CABALLERO Merci beaucoup. Je ne sais pas si, Graeme, tu veux rajouter quelque chose.

GRAEME BUNTON Graeme de l'Institut Beacon. J'essaierai d'être très bref, car Jeff a dit beaucoup de choses. Mais je dirais que justement dans le rapport INFERMAL, on met en exergue le fait que, justement, le fait de connaître son client semble alimenter l'usurpation d'identité. Et avec l'IA, les identités deviennent de plus en plus convaincantes. Donc je suis de moins en moins convaincu moi-même que l'IA sera une solution ou c'est peut-être une pièce du puzzle, mais je ne pense pas que cela nous permette de résoudre autant le problème que nous le pensons.

Et puis un autre élément qui me paraît intéressant et qu'il faudrait étudier en dehors du contexte de l'ICANN, c'est le lien entre fraude et abus pour voir s'il y a des outils technologiques que l'on peut utiliser à cet effet. Mais c'est vrai que cette semaine, je me suis entretenu avec une partie qui me disait que tous les abus, en fait toutes les utilisations malveillantes étaient passées par des cartes de crédit tout à fait légitimes qui ont été exploitées à mauvais escient. Donc voilà.

NICOLAS CABALLERO Désolé au Royaume-Uni. Je vous ai fait attendre.

NIGEL HICKSON Alors c'est vrai que c'est un domaine extrêmement complexe et clairement, il y a beaucoup de choses qui sont en train de se produire. Et nos adversaires travaillent d'arrache-pied sur de nouvelles modalités pour mener à bien leurs escroqueries, leurs actes de cybercriminalité. Moi, je crois que le rapport INFERMAL est extrêmement intéressant. Je me souviens, il y a quelques années, nous avons eu des discussions sur les enregistrements, notamment les enregistrements groupés. Maintenant, nous avons des éléments de preuve. Alors, je ne crois pas que cet après-midi, nous allions publier un avis du GAC en disant que tous les domaines doivent avoir une étiquette de prix de 100 $ ou plus. Non. Il y a quand même des questions de concurrence qui entrent en ligne de compte, d'autres enjeux également.

Et nous en avons parlé avec l'ALAC plus tôt. Il me semble que l'on pourrait effectivement ici lancer des PDP – des processus d'élaboration de politiques – concernant par exemple les enregistrements groupés dans certains domaines ou dans certaines zones plutôt lorsqu'il y a enregistrement groupé et que l'enregistrement est totalement gratuit. Eh bien, le bureau d'enregistrement offre peut-être un enregistrement gratuit pour un domaine particulier. Eh bien là, il semblerait qu'effectivement il faudrait poser d'autres questions. Est-ce que vous le faites parce qu'il y a un événement sportif et qu'on a besoin de tous ces

nouveaux domaines? Parce qu'il y a tout un processus en cours. Il y a une nouvelle école, que sais-je encore. Les usages sont multiples, mais je crois que nous devons effectivement faire un travail de recherche pour vraiment comprendre ce qui se passe sur le terrain.

REG LEVY

J'ai fait une analogie lors d'une présentation cette semaine concernant les enregistrements groupés en disant que en fait, c'est un peu comme le modèle de permis de conduire. Donc si vous avez par exemple un scooter, vous avez dans certains pays, on délivre des permis de conduire pour des personnes très jeunes. Mais si vous avez une semi-remorque, là par contre, pour avoir le permis de conduire, les critères sont beaucoup plus élevés. Pourquoi? Parce que vous pouvez porter atteinte à la vie humaine. Eh bien, de la même manière, nous voulons un modèle d'enregistrement groupé. Alors, c'est vrai que pour les bureaux d'enregistrement, on veut peut-être instaurer des normes qui sont beaucoup plus strictes.

Par exemple, on pourrait penser à des systèmes de garantie s'il y a abus sur vos enregistrements groupés. Eh bien, cette garantie sert à payer les frais et les préjudices. Cette garantie reste entre les mains des autorités. Ce serait une idée, une piste à suivre.

NICOLAS CABALLERO Merci beaucoup. Merci beaucoup à notre panel. Alors c'est vrai que cette discussion au sein du GAC a déjà commencé, mais j'aimerais maintenant passer la parole à Martina qui va nous expliquer les prochaines étapes.

MARTINA BARBERO Oui, alors nous avions l'espoir d'avoir une excellente séance et cette séance est excellente, mais nous voulions clore peut-être cette séance avec quelques questions à l'adresse du GAC. Nous aimerions recevoir les retours des membres du GAC concernant ce que vous avez entendu aujourd'hui. Quelles sont peut-être les constatations principales à tirer des différents exposés que nous avons entendus et les thèmes que nous avons couverts? Et puis, quelles sont les prochaines étapes concernant les utilisations malveillantes du DNS?

Certains ont déjà bien donné quelques pistes, mais nous voulons dans les cinq prochaines minutes vous entendre pour savoir quelles seraient les prochaines étapes idéales concernant cette thématique. Et comme équipe dirigeante, comme l'a demandé l'équipe dirigeante du GAC, nous pourrions également débattre d'éléments à incorporer au communiqué en aval de cette discussion par rapport aux attentes que vous avez en matière de futurs travaux, les éléments à prendre en considération pour le nouveau cycle. Rappelez-vous que, comme certains l'ont déjà mentionné, qu'il y a déjà eu des discussions au sein du GAC sur de possibles PDP – de processus d'élaboration de politiques – et au

sein d'autres communautés aussi, notamment l'ALAC qui souhaiterait pouvoir collaborer avec nous sur ce thème.

Donc nous avons peut-être deux ou trois minutes, Nico. Peut-être est-ce qu'on peut écouter les parties prenantes ici présentes?

NICOLAS CABALLERO Oui, je vois que le Royaume-Uni a levé la main. Nigel?

NIGEL HICKSON Non, c'est une ancienne main levée pour le Royaume-Uni.

NICOLAS CABALLERO Désolé. Trois minutes, Mesdames et messieurs, pour des questions, des observations, le plus rapidement possible, en ligne ou dans la salle. Je vous en prie, Monsieur, prenez un micro, quel qu'il soit.

DAVID HUGHES David Hughes au micro, unité constitutive représentante de la propriété intellectuelle. Alors, grande question. Alors, c'est vrai, nous avons constaté que certains ccTLD, mais pas nécessairement ça peut être des TLD aussi qui ont en fait des niveaux très bas d'utilisation malveillante du DNS. Que pouvons-nous apprendre? Quels sont les enseignements à tirer de ces expériences-là?

JEFF BEDSER Alors avant de pouvoir répondre à cette question, les gTLD doivent répondre à toute une série de règles. Les ccTLD n'en ont pas ou en

tous cas ces règles sont très variables. Ce faible niveau d'utilisation malveillante correspond aussi à un faible niveau d'utilisation et de croissance. Je dirais qu'il y a deux types d'utilisations malveillantes au niveau meta. Alors il y a les domaines enregistrés à des fins malveillantes et puis ceux qui sont détournés à des fins malveillantes. Et je crois que nous voyons en fait un grand nombre de domaines détournés au niveau des ccTLD, dans la plupart des études menées par rapport aux gTLD, en fonction du modèle, véritablement.

Donc je crois que, en fait, en se centrant sur les faibles niveaux à certains endroits, alors, il y a bien sûr certains TLD où il y a des taux les plus élevés, je ne veux pas nommer de noms. Donc vraiment, il y a beaucoup de gTLD qui enregistrent de très faibles niveaux d'abus. Donc là je ne sais pas très bien quoi répondre, je ne sais quelle réponse constructive apporter à tout cela.

GRAEME BUNTON Alors merci pour cette question. Il est très difficile de répondre à cette question. Revenons en fait au rapport INFERMAL. Alors on parlait de 73 caractéristiques, manettes comme on disait. Je ne pense pas qu'il y ait une seule caractéristique qui nous permette de tirer des conclusions. Et je ne pense pas non plus que les taux d'abus soient une erreur. Vous savez, les cybercriminels vont choisir un TLD pour l'une ou l'autre raison. Parce qu'une des manettes tourne, tout simplement parce que le bureau d'enregistrement ne connaît pas certaines failles, etc. Donc il faut

tenir compte de cette complexité et il faut également tenir compte des taux d'abus, mais aussi des taux d'atténuation et du taux moyen de l'atténuation dans toute cette chaîne des utilisations malveillantes.

NICOLAS CABALLERO Nico. Dernier commentaire. Eh bien, c'est pour Reg. À vous.

REG LEVY Oui, de la part du bureau, du groupe de travail des bureaux d'enregistrement. C'est intéressant. Je sais que certains ccTLD et d'autres vont en parler, je crois que c'est demain. Donc regardez l'emploi du temps pour avoir plus d'informations. Mais non seulement les ccTLD ont des politiques différentes, ils ont différents marchés et donc il y a des types d'abus qui parfois ciblent un ccTLD précis parce que c'est de cette manière qu'ils peuvent obtenir leurs clics. Donc il y a différents types de facteurs, comme l'a dit Graeme, à considérer, mais je vous encourage à participer à la séance ccTLD.

NICOLAS CABALLERO Merci beaucoup. Le Danemark rapidement, parce qu'on a déjà dépassé les temps.

FINN PETERSEN Finn Petersen du Danemark. Merci beaucoup de m'avoir donné la parole à la dernière minute. Je crois que c'est une bonne idée de

réfléchir aux ccTLD. Je sais que, dans un pays, les enregistrements ont été limités à cinq et il y a une enquête sur l'identité de ceux qui l'ont demandé. Si je réfléchis à ce qu'on a dit aujourd'hui, peut-être qu'il faudrait voir si on peut proposer une sorte de PDP sur les enregistrements groupés. Ceci permettrait de cibler davantage. Ceci permettrait peut-être davantage de possibilités d'adoption, de lancer le travail. Ce serait peut-être une solution assez facile pour le GAC.

NICOLAS CABALLERO Oui, effectivement, bonne idée. Donc cibler les choses. Et puis un délai de moins de cinq ans, ce serait déjà très bien. Merci beaucoup à tous, Reg, Graeme, Jeff, Tom, Leticia et Siôn. Merci. Nous allons faire une pause maintenant pour le déjeuner. Veuillez revenir dans la salle à 13 h 15. Merci beaucoup à tous. La séance est levée.

[FIN DE LA TRANSCRIPTION]