HYDERABAD – Session thématique des sujets d'actualité : Atténuation des risques d'abus dans les gTLD
Samedi 5 novembre 2016 – 13h45 à 15h IST
ICANN57 | Hyderabad, Inde

PERSONNE NON IDENTIFIÉE: Salle 3, 5 novembre 2016, de 13 h 45 à 15 h 00. Session de thèmes d'intérêt élevé : mitigation de l'usage malveillant des gTLD.

ALICE MUNYUA: Bonjour à tous. Bienvenue pour cette session qui a été organisée par le comité consultatif.

Je suis Alice Munyua. Donc, je suis la présidente du groupe de travail de sécurité.

Je vais commencer par présenter les membres du panel ici ou leur demander de se présenter.

S'il vous plait, donnez votre nom et le…

MICHELE NEYLON: Je suis Michele Neylon. Je suis un titulaire de noms de domaine.

BRIAN CIMBOLIC: Brian Cimbolic du registre.

STATTON HAMMOCK: Statton Hammock de registre.

CARLOS ALVAREZ: Carlos Alvarez de l'équipe RSS du personnel de l'ICANN.

GIOVANNI SEPPIA: Giovanni Seppia.

DENISE MICHEL: Denise Michel, unité constitutive commerciale.

ALLEN GROGAN: Allen Grogan.

DREW BAGLEY: Drew Bagley. Fondation de la sécurité de domaine.

BOBBY FLAIM: Bobby Flaim. FBI, groupe de sécurité publique.

FABIEN BETREMIEUX: Fabien Betremieux. Personnel de l'ICANN, soutien du GAC.

RICHARD ROBERTO: Richard Roberto, titulaire de registres.

ALICE MUNYUA: Merci à tous. Vous êtes les bienvenus.

Donc, ce groupe a été créé en 2015 lors de la réunion de Singapour et notre thème de référence principal se focalise sur les aspects de la politique de l'ICANN et les procédures qui impliquent la sécurité du public.

Donc, nous allons directement entrer dans le vif du sujet puisque nous n'avons pas beaucoup de temps et nous voudrions avoir le temps de passer à la discussion à la fin.

Nous allons nous baser sur l'atténuation de l'utilisation malveillante des gTLD. Nous allons fournir une mise à jour de la communauté de l'ICANN, des communautés consultatives pour l'atténuation des utilisations malveillantes du DNS.

Nous aurons aussi une mise à jour de la part de la communauté des SO et des AC pour connaitre les activités importantes, les informations importantes, l'efficacité de ces actions et les actions qui ont été mises en œuvre pour donc atténuer ces actions malveillantes. Cela va permettre à la communauté de

l'ICANN d'aborder des préoccupations et de présenter vos opinions, notamment pour donc les révisions et les activités.

Donc, notre ordre du jour, comme vous le voyez sur l'écran…

Nous allons commencer par une définition du groupe de travail de sécurité publique, Bobby Flaim.

Bobby Flaim, vous avez la parole.

BOBBY FLAIM: Merci Alice.

Je pense que lorsqu'on parle d'usage malveillant, nous avons un juge aux États-Unis qui a essayé de définir cela et je crois que dans le cas de la pornographie, je crois que c'est ce qu'on peut utiliser aussi sur tout ce qui concerne les utilisations malveillantes du DNS.

Nous avons ici une liste qui provient du groupe de travail de sécurité publique du GAC. Vous voyez ici les sauvegardes du GAC. Ici, cette définition comprend le pharming, l'hameçonnage, les réseaux zombies, etc. Mais c'est une liste beaucoup plus large.

Ces usages malveillants changent en fonction des pays. Nous devons considérer la loi nationale aussi, parce qu'elle s'applique, et un délit dans un pays peut ne pas l'être dans un

autre pays. De fait, il y a des exploitations d'enfants sur le DNS. Il y a des sites Internet qui sont utilisés pour le terrorisme, que nous voyons même à la télévision.

Donc, il y a différents types d'usage malveillant et il n'y a pas qu'une seule définition. Et je pense que c'est le plus important ici que nous devons considérer lorsqu'on analyse la question du DNS et de la sécurité publique du DNS.

Donc, nous espérons ou je sais que nous avons un très bon panel et un des objectifs ici, c'est d'avoir la perspective des opérateurs, l'opinion des opérateurs du DNS, c'est-à-dire les titulaires de registres, l'ICANN, les bureaux d'enregistrement. Donc, de façon à pouvoir savoir ce qui se fait, quelles sont les meilleures pratiques pour assurer qu'on peut prévenir et mitiger ou atténuer les usages malveillants du DNS dans l'environnement de l'ICANN?

Donc, nous pensons que ça va être très productif. Nous sommes heureux d'avoir cette conversation et cette discussion avec vous, avec les orateurs. Et donc, nous sommes heureux de cette participation.

Bien. Maintenant, je vais donner la parole à mon collègue Drew, qui va vous donner des exemples d'usage malveillant.

Donc, Drew.

DREW BAGLEY: Merci Bobby.

Donc, je vous parle du point de vue des usages malveillants et des tendances que nous voyons au niveau de notre fondation Secure Domain, qui est une fondation à but non-lucratif qui travaille dans le domaine des usages malveillants.

Vous savez que l'usage malveillant du DNS est quelque chose qui est important, non seulement dans le monde dans lequel nous vivons au niveau de l'ICANN, mais aussi parce que cela affecte des gens dans le monde entier en termes de victimes des dernières tendances de cyber-délit.

Et beaucoup des choses que nous entendons aujourd'hui commencent par quelque chose de très simple comme l'enregistrement d'un nom de domaine. Par conséquent, comme Bobby l'a dit, la définition technique de l'usage malveillant est très limitée. On pense à hameçonnage, le pharming, programme malveillant, etc. Donc, je vais me focaliser, en ce qui concerne les tendances, bien que l'usage malveillant du DNS puisse affecter bien d'autres choses, dans ce domaine.

Et une chose qui a été une tendance que tout le monde connait, depuis sept ans, depuis le [Inaudible] ces dernières années, c'est que l'usage malveillant du DNS a des ramifications financières

très importantes, beaucoup plus qu'auparavant. Et on voit qu'il est difficile d'isoler des victimes en particulier. Donc, nous en sommes à un point où ces usages malveillants du DNS affectent la stabilité du DNS d'une certaine façon et de son système.

D'autres tendances et d'autres menaces ces dernières années. Je pense que vous avez entendu parler de cela, c'était les systèmes de rançon qui prennent différents type de mécanismes avec le Cryptolocker et le Locky. Le compromis des courriels d'affaire et les réseaux zombies qu'on connait bien ces dernières semaines. On en a entendu parler.

Donc ici, quand on parle du système de rançon, du système pour imposer des rançons, il suffit de visiter un site Internet ou de cliquer sur un lien. À ce moment-là, on va vous demander de payer une rançon et cette rançon va affecter des organisations, des hôpitaux. Et on constate que dans le monde entier, c'est devenu un grave problème pour lequel des organisations, des compagnies peuvent perdre leur propriété intellectuelle de manière instantanée et leur capacité à organiser leur business lorsque leurs ordinateurs sont chiffrés. Et, à ce moment-là, les victimes paient ces rançons à ces cyber-délinquants pour récupérer leurs données et c'est pour éviter… Par exemple, en mars 2016, on a assisté à 56 000 infections, deux fois plus que ce qui s'était passé en 2015. On avait 23 000 infections par mois

l'année dernière et le montant d'argent payé dépasse les 209 millions de dollars.

Une autre tendance est que ce système de demande de rançon est offert comme service. Donc, on n'a pas besoin de savoir comment fonctionne ce système de codage. Il suffit de payer quelqu'un pour que cette personne s'occupe de faire cela à votre victime.

Ensuite, le système de compromis de courriel. Des exécutifs vont recevoir des courriels de hameçonnage qui leur paraissent tout à fait corrects, parce qu'ils paraissent venir de leurs employés et ce n'est pas le cas. Et dernièrement, lorsque des transactions financières ont lieu avec cet exécutif qui s'en occupe, il pense que c'est une demande légitime du département de trésorerie et donc, il accepte une transaction et cet argent est volé par les délinquants. Donc, on a plus d'un milliard de dollars de perte dans ce domaine.

Et ensuite, l'Internet des objets avec des réseaux de zombies, et de nouveau, des attaques cybernétiques. Ces tendances ont lieu de deux manières. On va attaquer un site Internet, mais ces cybers délinquants peuvent aussi enregistrer leur propre nom de domaine. À ce moment-là, récemment les tendances qu'on a constatées, c'est qu'ils vont voir des revendeurs qui acceptent des bitcoins. Ils offrent des services d'anonymisation. Et, à ce

moment-là, même si un revendeur est inclus dans ce… Si sa responsabilité au niveau des registres et des bureaux d'enregistrement a été critiquée, on constate qu'il y a une tendance intéressante qui a lieu au niveau de la périphérie, qui affecte les tendances de cyber-délits.

Bien. Maintenant je vais donner la parole au prochain orateur.

BOBBY FLAIM: Avant, je voudrais vous poser une question. En fonction des tendances qu'on voit au niveau du secteur du DNS et de l'utilisation des bitcoins, qu'est-ce que vous voyez comme solution possible pour lutter contre cette menace ?

DREW BAGLEY: Je pense qu'une des meilleures solutions serait une atténuation proactive.

Je pense qu'essentiellement, même si on n'a pas des bonnes données sur lesquelles on peut travailler, on… Lorsqu'il s'agit de l'anonymisation, il y a encore des données qui… On a tendance à utiliser les mêmes adresses courriel en permanence et cela met une certaine pression sur les fournisseurs d'anonymisation avec des preuves bien sûr pour démasquer et parfois même partager des données sur les titulaires de noms de domaine, de

façon à ce qu'on puisse commencer à voir et à utiliser ce système en permanence.

BOBBY FLAIM: Bien, merci. Notre prochain orateur sera Allen Grogan. Donc, Allen, vous avez la parole.

ALLEN GROGAN: Bien, merci. Donc, notre département s'occupe d'appliquer des contrats que nous avons avec les bureaux d'enregistrement et les registres. Nous essayons de lutter contre différents types d'usage malveillant.

Comme c'est la première réunion de ce type, pour cette réunion, je pense que ça va être un débat qui va durer en permanence pour le rôle de l'ICANN. Je ne vais pas essayer de répondre à cette question, mais je vais essayer de vous donner les dernières tendances dans ce domaine.

Donc, vu la nouvelle mission et les statuts constitutifs, il y a une tendance à dire que l'ICANN agit à l'extérieur de sa mission. Cette mission est une mission technique qui est liée à la coordination, à l'assignation pour faciliter leur système de routage, pour les protocoles, les nombres, etc. Donc, il y a aussi une nouvelle fourniture de service de l'ICANN pour utiliser l'identificateur unique de l'Internet et les services en

connaissance du fait que nous ne sommes pas… qu'ils ne sont pas réguliers.

Mais, à mon avis, je voudrais vous dire que pour appliquer le contrat existant, il y a une clause qui existait et qui existait avant la transition. Donc, avant 2016, et ces accords… J'ai établi dans cette diapo une série des clauses que contient notre contrat : les abus, le rôle de l'ICANN pour combattre ces abus, ces usages malveillants. En sachant que tout cela doit être dans la portée, dans la mission des statuts, doit être contenu dans les clauses de ce contrat.

Et, je vais maintenant donner la parole à Carlos qui va prendre la suite.

CARLOS ALVAREZ: Merci.

Donc, dans mon équipe, nous travaillons pour collaborer avec la communauté de sécurité et la communauté en général. Nous nous focalisons sur la partie contractuelle, pas seulement sur la partie contractuelle.

Nous nous focalisons aussi sur la partie coopérative et nous travaillons sur les activités malveillantes qui sont liées aux réseaux de robot, à l'hameçonnage et tout ce qui est à l'intérieur

de ces catégories n'est pas notre travail. Tout ce qui concerne la liberté d'expression, cela n'est pas notre travail disons.

Je voudrais me focaliser ici très rapidement sur certaines des choses que nous faisons, qui me paraissent importantes et que je vais mentionner ici.

Une des choses sur laquelle nous travaillons, c'est de fournir une formation aux forces de l'ordre dans le monde entier. Toutes les semaines, une personne de notre équipe va travailler dans le monde, dans une région, pour former des officiers de police sur les fondements du système DNS, sur des enquêtes à réaliser en profondeur, des questions qui sont importantes et qui concernent les menaces au système du DNS.

Un exemple récent, aux États-Unis, nous avons travaillé avec un centre de cyber-sécurité. Au Moyen-Orient, nous travaillons avec l'OIS, l'organisation des États américains. Nous avons aussi un centre en Europe. En Amérique latine, cette année, nous sommes allés dans différents pays : au Pérou, au Costa Rica, en Colombie. Donc, ce sont des exemples rapides.

Nous soutenons le travail de la communauté et de la sécurité et des forces de l'ordre. Nous fournissons des conseils concernant les enquêtes pour lesquelles ils travaillent, qui comprennent les sources du DNS. Ils nous posent des questions concernant le fonctionnement du DNS et nous répondons à ces questions. Des

fois, ils ne savent pas comment travailler dans le domaine du DNS et nous leur expliquons comment le faire. Nous les aidons à comprendre aussi le cadre de travail de l'ICANN.

L'enregistrement anti-abus qui se trouve dans le RAA pour préciser leurs attentes. Nous aidons aussi les forces de l'ordre, nos collègues qui, lorsqu'ils nous présentent des requêtes dans le cadre du processus de l'ICANN, qui s'appellent des requêtes de sécurité. C'est un processus de l'ICANN qui nous aide à résoudre les problèmes d'usage malveillant du DNS. Et donc, il y a eu des réseaux de… qui… malveillants il y a quelque temps qui ont été un grave problème et nous donnons des exemples actuels sur des événements et sur les cadres de sécurité en général. On nous demande de donner des conseils d'expert et nous les donnons.

Si vous posez des questions sur des problèmes de SSR, vous pourrez entrer en contact avec nous.

Certains des défis que nous constatons –il me reste cinq minutes et c'est peu, nous voyons des bureaux d'enregistrement, des registres qui ont différents systèmes. Différents systèmes de mise en œuvre, différentes ressources, différents niveau d'expertise et nous voyons aussi des plaintes des gens dans le secteur de la sécurité. Et des forces de l'ordre qui reçoivent des rapports d'usage malveillant qui ne sont pas clairs, qui ne

fournissent pas suffisamment d'informations, qui ne sont pas suffisants. Et, très souvent, ils ne sont pas non plus standardisés, normalisés, et donc ce sont des rapports d'usage malveillant qui rendent le travail encore plus difficile pour les bureaux d'enregistrement et les forces de l'ordre en général.

De même, nous voyons que les personnes ne comprennent pas vraiment les dispositions, tant du côté des plaignants que du côté des bureaux d'enregistrement. Ça arrive des fois et c'est donc approprié d'y faire allusion.

De même, il n'y a pas de politique uniforme à tous les registres et à tous les bureaux d'enregistrement en matière d'utilisation malveillante, c'est-à-dire qu'il y a certains qui pourraient avoir des politiques plus strictes que d'autres pour les titulaires de noms de domaine, c'est-à-dire qu'il n'y a pas d'uniformité. Il y a aussi une complication pour utiliser les données de recherche.

Nous espérons pouvoir avoir une définition claire de ce qui constitue une utilisation malveillante du DNS sous peu.

Certains secteurs de la communauté pourraient peut-être nous aider à mieux définir cela suivant le modèle de l'ICANN.

Et la recherche et la normalisation des processus d'information ou de signalisation d'utilisations malveillantes devraient également nous aider à renforcer ces initiatives. Merci.

BOBBY FLAIM: Merci Carlos. Je voulais redonner la parole à Drew qui va partir et qui voulait également nous expliquer les solutions d'atténuation de l'utilisation malveillante du DNS. Drew.

DREW BAGLEY: Merci Bobby. Je voulais tout simplement expliquer le rôle de l'ICANN et le rôle des autres parties prenantes dans cette initiative. Il est important que les bureaux d'enregistrement et les registres se partagent ces informations, que ce soit directement ou à travers des organisations tiers auxquelles ils font confiance. À travers ces processus de mise en commun et de partage d'information utile, il sera possible d'arrêter ces utilisations malveillantes et d'utiliser ce type de patron contre les personnes mêmes qui ont l'intention de perpétrer ces cas d'abus.

C'est vraiment très important pour la communauté d'assumer leur rôle. Il est important que chacun sache ce qu'il peut faire avec les données qu'il a en main et pour s'aider, pour qu'il y ait un système d'entraide qui nous permette de sécuriser l'Internet à travers la coopération.

BOBBY FLAIM: Merci Drew. J'ai quelques questions à poser à Allen et à Carlos. Maintenant qu'on est dans cette nouvelle ère après IANA, est-ce qu'il vous semble qu'il pourrait y avoir davantage de pression quant à l'autocorrection ou davantage de mesures de sécurités plus proactives ?

ALLEN GROGAN: Est-ce que vous pourriez expliquer ce que vous voulez nous demander par cela, ce que vous voulez dire?

BOBBY FLAIM: Dans ce nouvel âge d'un ICANN indépendant ou dans ce nouvel âge après IANA, est-ce qu'il vous semble que la communauté pourrait vouloir prendre le contrôle, d'agir davantage, qu'il y ait davantage d'autocorrection, d'autoréglementation, plus d'applications contractuelles puisqu'il n'y a plus de supervision d'aucune entité?

ALLEN GROGAN: Je suppose que, dans ce nouveau monde, la communauté va se demander davantage quel est le rôle de l'ICANN pour battre l'utilisation malveillante, l'utilisation abusive. Je ne suis pas sûr si la communauté va y arriver. Il y a différents points de vue, même dans les différentes unités constitutives de l'ICANN au sujet de la mission de l'ICANN, de ce qui est hors de la portée de

l'organisation. Et je pense que la PTI a impliqué un nombre de modifications à la mission et aux statuts constitutifs de l'ICANN. Et par conséquent, il y a davantage de pression sur nous pour faire plus que ce qu'on fait jusqu'à présent.

BOBBY FLAIM: Carlos, quel est votre avis ?

CARLOS ALVAREZ: Dans la communauté d'application de la loi et du SSR, nous voyons que les personnes veulent être plus actives en matière de mitigation ou atténuation des utilisations malveillantes. Donc, on devrait peut-être aborder la question et décider quel devrait être le rôle de l'ICANN dans ce contexte.

BOBBY FLAIM: Merci.

Nous allons maintenant Statton et Brian qui vont nous présenter les meilleures pratiques des registres et les stratégies d'atténuation des utilisations abusives. Brian va commencer.

BRIAN CIMBOLIC: Brian Cimbolic. Je suis vice-conseiller général du programme contre les utilisations malveillantes. Nous commençons à travailler sur nos politiques pour promouvoir l'utilisation

correcte du DNS et mettre une fin à l'exploitation infantile. Ensemble avec Afilias, on a commencé à travailler contre les utilisations abusives.

Quant aux mesures réactives, nous avons commencé à travailler avec un alias contre les abus, qui est contrôlé 365 jours par an, pour répondre aux plaintes, aux signalisations dans les huit à douze heures. Nous nous occupons directement des cas d'abus, soit moi-même, soit à travers mon équipe. On s'en occupe. En général, cela nous prend entre une et deux heures de commencer à enquêter sur la question, à nous pencher dessus, et autrement si c'est un peu plus compliqué, ça nous prend entre huit et douze heures.

Les requêtes sont typiquement présentées par les utilisateurs finaux ou par les agents d'application de la loi, ou même par les organisations. La plupart des signalisations des utilisateurs finaux ne constitue pas vraiment un cas d'utilisation abusive et ça ne correspond pas à notre politique contre les utilisations abusives.

Lorsque les personnes nous signalent des cas d'abus en général, ce sont des cas d'hameçonnage ou de pourriel, mais il y a également des signalisations concernant le malware.

En général, ce que nous faisons est de remettre les cas au bureau d'enregistrement. D'une part, parce que nous savons

quelle est la relation, le rapport, entre le bureau d'enregistrement et ses clients et ça leur donne également l'occasion d'entrer en contact avec le client pour voir s'il y a une autre explication. Pourquoi cette erreur est survenue ? Les bureaux d'enregistrement en général prennent les mesures relatives aux cas que nous leur faisons passer.

Mais en général, au moment de contacter les bureaux d'enregistrement, on les avertit que s'ils ne prennent pas des mesures, nous allons nous-même prendre des mesures suivant nos politiques anti-abus et mettre en suspension ce domaine. En général, on le fait. C'est le cas, parce que les bureaux d'enregistrement ne sont pas très efficaces. Une fois que le nom de domaine est supprimé, le même individu enregistre un autre nom de domaine pour l'utiliser aux mêmes fins.

Au moment de recevoir des signalisations des agents d'application de la loi, en général, cela sont abordés et adressés par le PIR pour essayer de rédiger même une définition d'une politique qui soit applicable, afin que le tribunal puisse décider de ce que peut faire le registre ou ce qu'il ne peut pas faire.

Nous avons également mis en place des mesures proactives pour atténuer la quantité d'utilisations abusives et c'est pour cela que nous avons beaucoup travaillé avec Afilias. Nous avons enregistré nos différents patrons inhabituels. Donc, ces

procédures nous permettent d'identifier les cas où le comportement ne suit pas le comportement habituel des DNS. Ça ne veut pas dire que c'est nécessairement un cas d'abus, mais ça nous fait regarder et enquêter si le nom de domaine pourrait être ou pas un pourriel, ou un autre type d'abus.

Nous recevons également des rapports sur les différents enregistrements et nous faisons des références croisées avec les différentes listes noires. Ça ne veut pas nécessairement dire qu'il y ait un problème ou un abus, mais ça nous fait regarder s'il y a des activités qui ne sont pas correctes.

Au cas où on trouverait des abus potentiels ou probables à travers ces mesures, nous suivons les mêmes mesures que nous avons mises en place pour les mesures réactives. Donc, on contacte le bureau d'enregistrement; on lui donne l'occasion de contacter le titulaire du nom de domaine. Si le bureau d'enregistrement ne prend pas de mesures, le nom de domaine est mis en suspension.

Donc, cela dit, je redonne la parole à Statton.

STATTON HAMMOCK: Namaste. Merci d'être là. Je suis Statton Hammock. Pour ceux qui ne connaissent pas Rightside, c'est un service de noms de domaine qui est intégré. Nous travaillons avec les registres et les

bureaux d'enregistrement. Les opérateurs de registre travaillent avec quarante TLD.

Et donc, comme vice-président des politiques et de la partie des affaires, j'ai accès à différents usages malveillants du côté des registres et du côté des bureaux d'enregistrement. Je vais vous donner un petit peu une idée de ce que nous rencontrons pour vous donner un petit peu un panorama au niveau des gTLD.

Lorsqu'on parle d'usage malveillant, je veux que ce soit clair que, lorsqu'on parle d'effort contre ces usages malveillants, on parle d'une série de choses. Certaines sont nécessaires pour les registres en accord avec l'ICANN et c'est là, la mise en œuvre des mécanismes de protection des droits, qui ont été conçus et développés pendant la genèse du programme des nouveaux gTLD qui comprend la période du *sunrise*, la période UDRP et la période de processus de résolution de différends, la question de processus de différentes post-délégations, etc. En tant que registre, nous avons aussi une série d'engagements envers le public que nous devons inclure, qui sont nécessaires. Certains viennent de la communauté multipartite, d'autres des conseils du GAC et d'autres sont aussi mis en œuvre au niveau de notre accord de registre.

Et ensuite, il y a ce que j'appelle les efforts plus volontaires dans le cadre de l'industrie qui ne sont pas requis au niveau

contractuel, que les registres et les bureaux d'enregistrement mettent en œuvre d'eux même pour combattre les activités illégales sur Internet.

Donc, une série de registres offre des systèmes de protection de domaines, des listes de blocage pour protéger les noms de marques. Il y a un système donc de plainte, des processus dans lesquels on a prolongé la période de plainte pour que les propriétaires de marque puissent lutter contre les enregistrements qui portent atteinte à leurs marques. Et d'autres efforts incluent le travail sur un cadre de sécurité et dans lequel le groupe de partie prenante de sécurité travaille pour trouver des processus et des manières d'aborder ces abus.

Ensuite, quelque chose qui va au-delà de ces efforts volontaires qui concernent la politique de la communauté de l'ICANN, ce sont des initiatives de registres et de bureaux d'enregistrement individuels qui nous aident à lutter contre différents types d'usages malveillants.

Nous travaillons avec des groupes pour lutter contre les problèmes de pornographie auprès d'enfants. Il y a une série d'initiatives avec des associations de noms de domaine, des associations commerciales qui représentent l'industrie du nom de domaine qui travaillent avec les principes et les meilleures pratiques pour lutter contre les pharmacies illégales, les

attaques contre la sécurité, d'autres types d'attaques malveillantes.

Donc, c'est un petit peu le paysage des efforts que nous faisons pour lutter contre ces abus. De notre côté, nous avons plus d'un demi-million de noms de domaine enregistrés de TLD. Nous avons trois sources de rapport d'abus que nous utilisons pour nos contrôles au niveau quotidien. Nous avons trois TLD qui sont très réglementés, c'est-à-dire qu'ils sont très… Ce sont des noms de domaine professionnels.

Nous n'avons aucun engagement d'intérêt public et de problème ou de conflit dans ce type de domaine. Nous avons quarante-deux procédures lancées aux États-Unis. Donc, nous voyons qu'il y a une tendance cohérente avec les plaintes qui existent au niveau de l'ICANN et au niveau du bureau de conformité de l'ICANN en termes d'abus.

Dans la plupart des cas, il s'agit d'hameçonnage, de programmes malveillants, ce type de choses, pourriels, mais très peu de choses sont faites au niveau des contenus des sites et des choses qui pourraient être le cas dans les TLD. Dans certains cas, ce sont des registres pour répondre à ces plaintes. Certaines actions sont prises par les registres, d'autres par les bureaux d'enregistrement.

Finalement, de nouveau pour répéter un petit peu, vu le nombre de noms de domaine qui sont enregistrés maintenant, on a un niveau d'abus qui est quand même assez bas, qui a été rapporté.

Donc ça, c'est pour voir le bon côté des choses et mon collègue ici va vous parler un petit peu plus de tous ces aspects-là.

BOBBY FLAIM: Merci Stan. Je suis Bobby Flaim. Merci Statton et Brian. Je voulais vous demander, vous poser une question. Est-ce que vous avez des informations que vous diffusez parfois lorsque vous rencontrez des acteurs particuliers?

STATTON HAMMOCK: Oui. Au niveau des bureaux d'enregistrement, mon équipe qui travaille avec la conformité va partager des informations sur les bureaux d'enregistrement pour les mauvais acteurs. Lorsque nous constatons qu'il y a un mauvais acteur qui est en train d'essayer de pirater des noms ou de mettre en place une activité malhonnête à travers, nous essayons d'avertir les différents bureaux d'enregistrement de ces nouveaux acteurs.

Mais rien de formel puisque nous savons que c'est une question de bonnes pratiques tout cela.

BOBBY FLAIM: Bien. Merci Statton. Maintenant, nous avons Giovanni Seppia.

Excusez-moi. Giovanni Seppia. Oui, une question ?

PERSONNE NON IDENTIFIÉE: Bonjour, je suis [inaudible]. Je suis un boursier de l'ICANN. J'appartiens aussi au NomCom. J'ai une question sur les listes noires. C'est une… Vous avez parlé… Vous avez parlé de listes noires. Où est-ce que vous trouvez ces sources pour donc alimenter ces listes noires ?

BRIAN CIMBOLIC: D'accord. Merci pour votre question. Beaucoup de ces listes sont disponibles et il y a des époques où ces listes provoquent certaines sensibilités. Une des raisons, une des manières pour nous d'atténuer les risques possibles par rapport à cela, c'est de se référer au bureau d'enregistrement à travers le titulaire de nom de domaine et qui aura la possibilité de dire pourquoi nous en sommes, pourquoi nous en sommes arrivés à cette conclusion et qui peut dire qu'il n'a pas d'usage malveillant.

PERSONNE NON IDENTIFIÉE: Donc, je dois partir du principe que ces listes sont disponibles sur Internet.

BRIAN CIMBOLIC: Oui, tout à fait.

BOBBY FLAIM: Bien. Nous allons reprendre, prendre une question de plus. Mais ensuite, si vous voulez bien, nous allons vous demander de garder vos questions pour la fin de la présentation de façon qu'on ait le temps de faire les présentations, puisque nous avons une trentaine de minutes à la fin de ces présentations pour les questions.

Bien, allez-y.

KIRAN MALANCHARUVIL: Merci Bobby.

Comme compagnie qui travaille pour la protection des marques, je vous dirais que je pense que ce n'est pas nécessairement juste de dire cela, parce que nous ne rapportons pas des usages malveillants. Des fois, il y a des usages malveillants que nous rapportons ou que nous ne pouvons pas rapporter, parce que nous ne savons pas où le faire. Comme nous avons une politique d'abus qui est très stricte et comme vous êtes très strict dans votre interprétation des abus, nous sommes une compagnie juridique – je ne pense pas que nous sommes le seuls dans notre secteur, nous ne pouvons pas soumettre nos plaintes d'abus à vous. J'aimerais que vous nous aidiez comment, à savoir

comment, combien de noms de domaine sont rapportés dans tous les systèmes – au niveau des ISP, au niveau des bureaux d'enregistrement qui sont associés avec vos registres.

Ce serait beaucoup mieux comme donnée pour nous que d'avoir ce type de données pour savoir quels types d'abus sont présentés, pas seulement à vous en tant que registre.

STATTON HAMMOCK: Merci. Les données que je vous montre proviennent des abus rapportés au niveau le plus bas. Cela vient de tous, c'est-à-dire ce que nous recevons au niveau des registres, des sites Internet ou des plaintes reçues par l'ICANN.

BOBBY FLAIM: Merci. Nous allons passer maintenant, nous allons donner la parole à Giovanni.

GIOVANNI SEPPIA: Merci Bobby. Giovanni Seppia. Donc, je suis le directeur d'EURid, opérateur de registre.

Et la première diapo que je vais vous présenter est pour montrer du point de vue technique et administratif.

EURid est un .eu, un ccTLD. Nous appartenons à la famille des ccTLD. Nous sommes très réglementés puisque nous avons deux

réglementations de l'Union européenne, une qui date de l'année 2001 et la deuxième qui contient les règles de politiques publiques qui date de l'année 2004. Donc ces deux réglementations contiennent une clause de base qui est que .eu est un nom de domaine qui peut être enregistré seulement par des résidents de l'Union européenne ou par des pays qui appartiennent à la zone de la Communauté européenne. Donc, nous servons un marché de trente-et-un pays et nous avons un peu plus de 3,8 .eu, noms de domaine .eu qui sont enregistrés.

Donc, c'est important pour nous de souligner et que nous avons un environnement multilingue aussi puisque nous travaillons en alphabet cyrillique aussi.

Nous avons mis en place une série de mesures pour protéger nos noms de domaine, d'un point de vue administratif. Donc, nous avons le DNSSEC, nous avons un système qui s'appelle *homoglyph bundling* qui a été créé il y a quelques années pour s'assurer que les noms de domaine IDN lorsqu'ils sont enregistrés si ce sont des noms de domaine qui sont regroupés et réservés. Par conséquent, il n'est pas possible d'enregistrer les noms de domaine qui se ressemblent les uns les autres et comme cela, nous protégeons les titulaires de noms de domaine de problèmes possibles qui pourraient surgir de noms de domaine qui ressemblent beaucoup à leur propre nom de

domaine et pourraient être enregistrés par d'autres titulaires de noms de domaine.

Nous avons aussi lancé un système qui s'appelle politique de correspondance de scripte et pour que les écritures latine ou cyrillique fonctionnent chacune dans des catégories différentes. Tout cela dans l'environnement .eu.

Ce que nous avons mis aussi en œuvre il y a quelques années, c'est ce que nous appelons le plan de qualité du WHOIS. Les autorités d'EURid et du registre .eu sont très limitées par ces réglementations et par conséquent, nous devons travailler, nous devons réfléchir pour voir comment nous pouvons faire dans le cadre de ces réglementations.

En général, nous mettons en place des actions lorsque nous recevons des plaintes concernant les usages malveillants liés à notre nom de domaine .eu et très souvent, nous comptons sur la coopération de nos bureaux d'enregistrement. Il y a un plan de qualité qui a été développé en collaboration avec nos titulaires de noms de domaine et avec le Conseil consultatif des titulaires qui nous donnent des conseils pour développer donc ce plan de qualité.

Ce que nous faisons, nous vérifions l'enregistrement, les données d'enregistrement et nous vérifions ces données d'enregistrement au quotidien. Les données d'enregistrement

sont vérifiées directement par EURid ou à la demande d'une tierce partie, certaines par les forces de l'ordre par exemple.

La vérification concernant les vérifications de ces adresses dans le nom de domaine .eu ne peut être faite que par des résidents de nos pays et la vérification des adresses est faite dans les bases de données de tierces parties ou sur Google.

Pour vous donner des statistiques, en 2015, nous avons effacé plus de 30 000 noms de domaine, parce qu'ils ne répondaient pas à ces critères tel que cela a été établi par ces réglementations au niveau européen.

Ici, vous voyez une liste des différentes autorités qui existent dans la région, comme par exemple le cert.eu. Nous avons un protocole d'accord, nous avons une coopération et un dialogue avec eux. Certains de mes collègues dans ce panel ont mis l'accent là-dessus, parce que ça demande beaucoup d'éducation pour qu'ils comprennent ce que nous pouvons faire dans le cadre de nos réglementations, de notre politique publique et de nos règles dans ce sens et comment nous pouvons agir en coopération avec eux ou en coopération avec notre réseau de bureaux d'enregistrement crédités.

Ensuite, nous avons la prévention de l'usage malveillant que nous développons actuellement. C'est un système très intéressant, une analyse que nous faisons en coopération avec

une université et cela vise à prédire des usages malveillants possibles et à déléguer à la demande des bureaux d'enregistrement pour les noms de domaine qui pourraient donner lieu à des usages malveillants.

Nous en sommes au début de ce projet. C'est un projet qui a seulement commencé il y a un an et nous espérons que nous allons pouvoir appliquer les principes de prévention plutôt que régler les problèmes une fois que les problèmes surgissent.

Je répondrais à vos questions si vous en avez.

BOBBY FLAIM: Merci beaucoup, Giovanni. On dirait que vous travaillez beaucoup sur l'atténuation des cas d'abus. Est-il possible de mesurer la quantité de ressources, combien de ressources vous utilisez pour faire ce travail ?

GIOVANNI SEPPIA: C'est une bonne question. Dans les dernières années, on s'est rendu compte qu'on avait décidé d'avoir le .eu et de le promouvoir comme un nom de domaine de qualité. Ce qui veut dire qu'on a investi davantage de ressources pour le montrer comme une ressource de qualité et un nom de domaine de qualité. Donc, nous travaillons beaucoup sur l'atténuation des cas d'abus.

Notre équipe juridique en ce moment est formée par trois effectifs qui seront quatre d'ici peu, et deux de ces personnes sont exclusivement consacrées au plan de vérification du WHOIS, au plan de qualité et quant à mon équipe, nous travaillons avec toutes les équipes européennes. Et l'équipe juridique assure également ce rôle de liaison avec les bureaux d'enregistrement. Donc, je voudrais souligner que pour le registre, il est important d'avoir une bonne coopération avec les bureaux d'enregistrement.

Dans cette dernière année, nous avons eu de très bons exemples de mesures concrètes qui ont été prises par les bureaux d'enregistrement contre les revendeurs qui faisaient abus du système. Certaines de ces actions ont même abouti à la conclusion du contrat, à la conclusion anticipée du contrat, parce que justement il y avait eu des cas d'abus de la part du revendeur. Cela a un impact sur tout le système d'enregistrement.

Donc, c'est un élément clé pour lutter contre les cas d'abus.

BOBBY FLAIM: J'ai une autre question là-dessus au niveau de votre travail avec les bureaux d'enregistrement ?

Est-ce que vous avez une vision spécifique par rapport à ce qu'il faut faire avec le bureau d'enregistrement ?

GIOVANNI SEPPIA: Bien. Lorsque nous voyons un cas d'attaque d'un nom de domaine avec des données d'enregistrement, que ce soit avec l'adresse d'email ou le nom du titulaire du nom de domaine ou d'autres données d'enregistrement, et que ces utilisations des données semblent être un peu bizarres, nous contactons par email le titulaire du d'enregistrement, le titulaire du nom de domaine et nous fournissons les données qui ont été enregistrées pour qu'il vérifie s'il a utilisé ces données. Donc, on s'assure en même temps que le bureau d'enregistrement ait également l'occasion de contacter le titulaire du nom de domaine pour résoudre ce problème, puisque c'est eux qui sont la voix qui nous connectent avec les enregistrements du .eu.

Dans la plupart des cas, les personnes ne veulent pas vraiment faire cela, parce que pour eux, ça veut dire que c'était une charge supplémentaire que de fournir des ressources pour assurer ces travaux. Mais en ce moment, nous travaillons avec tous nos bureaux d'enregistrement; ils nous ont tous aidé à assurer la qualité de notre domaine à travers ce plan de qualité des données WHOIS.

BOBBY FLAIM: Merci Giovanni. Nous allons donner la parole à Michele.

MICHELE NEYLON: Merci. Je suis un bureau d'enregistrement et un fournisseur d'hébergement aussi.

Je voudrais adresser certains des défis auxquels doivent faire face les fournisseurs de service et les bureaux d'enregistrement.

Ceux qui m'ont précédé parlaient des données qu'ils ont à leur disposition et des défis auxquels ils doivent faire face. Des fournisseurs d'hébergement, les FSI, les bureaux d'enregistrement, nous avons quelques problèmes, surtout par rapport aux rapports que nous avons avec les autorités.

Dans ces dernières années, nous avons eu quantité d'initiatives dans les différentes régions au sein de la communauté FSI pour essayer d'améliorer la qualité des rapports en termes généraux en matière d'abus, mais on n'y est pas arrivé pour l'instant. On n'a pas de normes qui évaluent la qualité de cela. Il y a des personnes qui se plaignent du manque de normes par rapport aux réponses.

Donc, si vous voulez informer de ce type d'abus, nous signaler ces abus, je dirais qu'il faut que vous informez du type d'abus qui vous semblent être en train de voir. Donnez-nous des exemples clairs de cet abus.

Aujourd'hui, lorsque je voyais notre tableau de bord qui fait le suivi des cas d'abus, on voyait qu'il disait : le domaine X est appliqué dans l'abus. Et c'est très utile. Il va falloir que l'on décide exactement quel est le type d'abus auquel cela correspond bien sûr.

Mais d'autre part, lorsqu'on parle d'utilisation malveillante et qu'on veut avoir une portée spécifique du point de vue des bureaux d'enregistrement et en tant que fournisseur d'enregistrement, nous ne voulons pas nous retrouver dans une situation où on nous demande d'agir en tant que juge, jury et exécutionnaire, c'est-à-dire qu'on veut avoir des orientations claires par rapport aux plaintes et pourquoi cela relève de notre autorité de nous occuper. Qu'est-ce que vous voulez que nous fassions ?

Quant aux botnets, malware, en termes généraux, je dirais que pour la plupart de nous, ça n'a aucun intérêt d'avoir ce type de contenus pour les noms de domaine qui sont liés à nous. Si on agit en tant que bureau d'enregistrement par contre, les noms de domaine ne correspondent pas à un outil spécifique.

Je pourrais très bien, c'est-à-dire je pourrais très bien éliminer le nom de domaine, mais je ne peux pas supprimer des parties de ce nom de domaine ou mettre en suspension une partie seule de ce nom de domaine.

On doit tout simplement interrompre tous les services qu'on fournit pour ce titulaire de noms de domaine. Donc, il faut comprendre ce qu'on peut faire, quelles sont les limites de ce que nous pouvons faire.

On a beaucoup parlé des révisions ici à Hyderabad et je vois qu'il y a des membres du CCRT qui sont ici. Les membres de cette équipe travaillent sur une révision qui comprend l'utilisation malveillante et j'espère qu'ils pourront nous donner des données spécifiques, des données concrètes qui seraient utiles pour nous.

Il nous faut savoir s'il y a un rapport par exemple entre les noms de domaine dans des extensions particulières et leur utilisation ou s'il y a un rapport entre les stratégies de tarification? Les données seraient utiles, on n'a pas besoin uniquement de théories.

En tant que bureau d'enregistrement, nous voulons travailler avec le reste de la communauté, mais il faut savoir que ce que nous pouvons faire a des limites. Et si nous vous demandons davantage de détails, c'est pour essayer de comprendre quelle est la plainte, pourquoi vous vous plaignez ou quel est le problème. Je n'ai pas beaucoup d'autres choses à dire.

Depuis notre point de vue en tout cas, ce qui est intéressant, est la qualité des rapports eux-mêmes. Si la communauté peut

travailler ensemble pour améliorer ces rapports, ce sera utile pour que l'on puisse avancer vers quelque chose de plus positif.

Merci.

BOBBY FLAIM: J'ai une question, Michele. Lorsque vous parlez des spécificités et que vous voulez des détails, est-ce que vous avez des exemples de sécurité opérationnelle ou de fournisseur de ce type de services, ou d'une unité constitutive spécifique qui vous donne ce type de détails pour vous permettre d'agir?

MICHELE NEYLON: Bien sûr, Bobby. C'est une très bonne question.

Dans le cadre de l'application de la loi par exemple, il pourrait peut-être, il pourrait peut-être que l'on préserve les enregistrements ou les accès si on parle de l'hébergement, ou si on agit en tant que bureau d'enregistrement, peut-être que vous visez à ce qu'on mette en suspension le DNS.

Ça dépend du cas par cas bien sûr, mais plutôt que de venir nous dire qu'il y a un problème, ce serait utile de nous dire : bon, on a ce problème, on voudrait que vous fassiez ça et ça.

Il y a également une autre question commune qui correspond à la juridiction. Ma société est irlandaise. Vous êtes américain, et

même si on s'adore, si vous m'envoyez des réglementations qui correspondent à la loi américaine, je ne vais pas les suivre.

Si vous m'envoyez des lois qui correspondent à ma juridiction, c'est très bien. Mais par exemple, pour le DMCA, le DMCA n'est pas une loi contraignante pour moi. Je suis une société de droit irlandais et donc, je ne peux pas suivre vos réglementations. Donc, je vais ignorer votre rapport et je vais rien faire par rapport à cela.

Bertrand de la Chapelle a un projet sur la juridiction dans lequel il travaille sur des modèles de rapports. Donc, par exemple, il a compris la question de la juridiction dans le domaine de son travail. Quelles sont les lois actuelles concernant la juridiction par exemple? Quelles sont les mesures attendues?

Donc, plus le rapport est spécifique, plus il est facile pour nous de prendre une décision pour voir si nous avons suffisamment d'informations pour pouvoir prendre des mesures ou s'il nous faut vous le remettre pour vous dire c'est très bien, mais vous n'êtes pas dans notre juridiction. Vous ne nous avez pas donné suffisamment de détails pour pouvoir agir.

BOBBY FLAIM: Merci Michele. Je sais que c'est un gros problème lorsqu'on parle d'utilisation malveillante des DNS, puisqu'on n'appartient

pas aux traités internationaux ou qu'on n'a pas des conventions de crime international. Donc, lorsqu'on parle de conflit, de droit et des complications du système juridique qu'on a aux États-Unis où on applique le MLAT – Traité d'assistance mutuelle – pour les services juridiques.

Donc ce type de complications sont très réelles, très spécifiques et il nous pose de vrais défis.

Je voudrais maintenant donner la parole à Denise qui est la dernière présentatrice. Après cela, nous allons aborder vos questions.

DENISE MICHEL: Merci Bobby.

Je viens ici mettre en valeur les défis pour les sociétés au niveau mondial et pour les utilisateurs et les clients également.

Il y a peu de compagnies qui suivent la même échelle et qui aient les mêmes concurrents que Facebook et son groupe sociétaire. Nous travaillons beaucoup pour protéger nos utilisateurs et pour aider à sécuriser l'Internet.

Les noms de domaine sont à la fois une source d'utilisation malveillante et la clé pour dépister, dissuader et prévenir ces utilisations malveillantes sur nos plateformes mondiales.

D'habitude, les personnes ne font pas attention ou les personnes dans la communauté de l'ICANN ne savent pas qu'un seul domaine malveillant peut comprendre différents FQDN.

Donc, un seul nom de domaine malveillant – je répète – comprend différents FQDN qui, à la fois, atteignent ou ciblent une quantité exponentielle d'URL et notre plateforme qui est mondiale finit par avoir beaucoup d'ordres de magnitude atteintes pour nos utilisateurs.

Donc, j'ai une présentation qui est publié sur la page de cette séance et qui explique les différents éléments clés des RAA et des outils qui sont également inclus dans le RA, les outils qui peuvent utiliser et les obligations contractuelles qui peuvent aider à atténuer les cas d'abus.

Donc, bien sûr, les bureaux d'enregistrement et les registres peuvent prendre des mesures pour essayer d'arrêter ou d'atténuer ces fonctions malveillantes.

Mais il devrait y avoir également un encouragement qui les fasse faire cela. L'idée est de protéger l'utilisateur final tout en étant positif pour l'écosystème du DNS.

Donc, je voudrais vous donner un exemple de comment faire cela.

Il y a quelques mois on a enregistré deux noms de domaines : login-account.net et video.net. Donc, il y avait des détails d'enregistrement qui étaient compris dans les deux. Bon. Il y a ici les données d'enregistrement de WHOIS pour l'un de ces domaines. Ce registre a été utilisé pour enregistrer ces deux noms de domaine.

Comme vous voyez, ce sont des informations de Facebook partout, y compris notre adresse email, à l'exception des serveurs de noms.

Ces deux noms de domaine ont été utilisés pour lancer des malware d'hameçonnage, des attaques contre des millions d'utilisateurs. On a rapidement détecté cela et on a bloqué ces démarches et on a signalé cela au bureau d'enregistrement et à l'équipe de conformité de l'ICANN.

Le bureau d'enregistrement n'a pas vérifié l'enregistrement de ces deux noms de domaine qui utilisaient notre adresse email. C'aurait dû être vérifié à travers l'adresse email. Mais nous nous sommes plaints, nous avons soumis cette plainte à l'équipe de conformité contractuelle de l'ICANN, qui a ouvert et fermé le dossier dans les 24 heures sans apporter de modification aux noms de domaine ou au registre WHOIS.

Ça nous a pris deux mois et des dizaines de communication pour pouvoir suspendre ces deux noms de domaine. Malgré leur

reconnaissance – la reconnaissance du bureau d'enregistrement – que ce registre WHOIS avait été utilisé pour un abus ou à des fins malveillantes, cela vous montre que le système a ses propres défaillances.

Si le bureau d'enregistrement ne vérifie pas l'enregistrement au moment de l'enregistrement, le système ne va pas fonctionner. On a donc besoin d'avoir des bureaux d'enregistrement qui fassent attention aux données d'enregistrement. S'il ne le fait pas, il va falloir que l'on prenne des mesures immédiates pour donner remède à ce manquement au RAA. Ici, onlineNIC a insisté que l'on ait l'approbation des titulaires des noms de domaine pour modifier le WHOIS alors que c'était des enregistrements qui utilisaient des données de quelqu'un d'autre à des fins malveillantes.

Le système échoue si l'équipe de conformité contractuelle de l'ICANN conclut un dossier sans résoudre le problème et puis, prend « des mesures d'application coopérative » avec le bureau d'enregistrement qui ne se conforme justement pas à ces règles.

En tant que plateforme globale, Facebook comprend bien qu'il y a des cas d'abus qui ne sont pas arrêtés, que les procédures existantes ne sont pas parfaites. Mais notre communauté devrait exiger que toutes les parties mettent en place des efforts raisonnables pour pouvoir mettre en place les procédures

existantes et que lorsqu'on a des défaillances procédurales, on doit les rectifier dans des courts délais. Ça ne devrait pas nous prendre deux mois de résoudre des cas d'utilisation malveillante de noms de domaine. Et l'ICANN de sa part doit aborder les défaillances procédurales ignorées ou habituelles à travers l'équipe de conformité contractuelle.

Ce n'est donc pas la peine de réinventer la roue. On a des politiques pour la prévention d'abus et des obligations contractuelles qui existent déjà et qui sont utilisées de manière appropriée par la plupart des bureaux d'enregistrement et les registres dont certains sont ici. Mais il faut qu'on s'assure, que l'on s'assure que tout le monde l'utilise correctement.

BOBBY FLAIM: Merci Denise. Il nous reste douze minutes pour les questions. Je sais, Peter, je m'excuse. Vous êtes le premier intervenant. Je sais que vous aviez une question. Donc, si quelqu'un d'autre a des questions, veuillez vous rapprocher du micro. Nous avons jusqu'à 15 h 00. Merci.

PETER VERGOTE: Merci Bobby.

Bonjour à tous. Je suis Peter Vergote. Je suis directeur d'un CENTR, d'une organisation qui a un ccTLD.

Je voudrais répondre à une question que Michele a soulevée : il semble qu'il y ait un manque de compréhension des différents faits qui donnent lieu à une augmentation ou à une baisse des abus dans un domaine spécifique.

Nous avons fait une étude il y a un mois. Il y a une série de choses qui sont disponibles. Je vais vous les envoyer par Twitter, comme ça vous pouvez les partager si ça vous intéresse.

Je sais que certains ont fait des recherches détaillées sur des facteurs spécifiques. Je ne sais pas si ces informations sont publiées déjà, mais je sais qu'ils ont l'intention de publier cela bientôt. Donc, premier point. J'espère que ça va vous aider.

Deuxième point. C'est important pour cette discussion pour les Européens surtout et il s'agit de la discussion qui a eu lieu dans le cadre du marché numérique de la révision de la protection des consommateurs et des réglementations dans ce sens. La proposition est d'aider à résoudre la protection des consommateurs en fermant des domaines directement.

Et le problème qui apparait ici, et c'est quelque chose qui me parait un peu compliqué et dans ce panel aussi, c'est le manque de vocabulaire commun pour définir ce dont nous parlons, notamment quand il s'agit des forces de l'ordre en Europe, des gouvernements. Je pense qu'il faut commencer à harmoniser tout ce vocabulaire. Je suggérais à ce panel de voir s'il y a la

possibilité, en tant que ccTLD européen et la communauté dans son ensemble, de régler ce problème.

Je sais que c'est un problème compliqué, mais nous allons devoir régler ce problème tôt ou tard.

Merci.

Merci. Mike?

BOBBY FLAIM: Est-ce que quelqu'un a des commentaires à ce propos? Michele, allez-y.

MICHELE NEYLON: Merci. Oui, c'est très utile, ces statistiques. Le problème, c'est que je parlais des gTLD, mais de toute façon, je vous remercie. Avant que quiconque le dise, je suis tout à fait d'accord avec vous.

BOBBY FLAIM: Merci.

MICHAEL PALAGE: Une question : est-ce que l'ICANN, est-ce que la partie de conformité de l'ICANN reçoit de rapports d'usage malveillant fournis par des tierces parties?

Je pose cette question, parce que j'ai fait une recherche pour essayer d'identifier quelles sources l'ICANN utilise, et il m'a semblé qu'il y avait des lacunes. Donc, je pense… Je voudrais savoir s'il y a un rapport… L'ICANN parle de confidentialité et ne fournit pas ces réponses. Donc, je voudrais savoir quelles sont les ressources que le personnel de l'ICANN et l'équipe de sécurité utilisent et donnent à votre ou met à disposition de votre équipe pour faire votre travail?

ALLEN GROGAN: Bien. Je ne sais pas je peux vous répondre.

BOBBY FLAIM: La partie de conformité de l'ICANN ne s'occupe pas vraiment de cela. Peut-être que les représentants de l'équipe ici pourraient vous répondre.

CARLOS ALVAREZ: Vous parlez des déclarations d'usage malveillant?

MIKE PALAGE: Ce que j'essaye ici de vous dire, c'est qu'hier, Margie, dans le groupe de cc, a parlé de la façon dont ils allaient réaliser une analyse des usages malveillants des gTLD dans le marché. Et donc si vous faites une analyse historique par rapport à ce qui se

faisait dans le passé et si vous comparez à ce qui se fait aujourd'hui, quelles sont les bases de données collectées pour faire cela? Je pense que quelqu'un a dû recueillir ces données, non?

CARLOS ALVAREZ: La question devrait être posée aux ccTLD.

MICHAEL PALAGE: Donc, que fait votre équipe? Qu'est-ce que vous faites? Est-ce que vous pouvez nous montrer ce que vous faites pour pouvoir faire votre travail? Est-ce que vous partagez avec l'équipe de conformité ou vous travaillez en silo à ce moment-là? C'est ça la question : est-ce qu'il y a une communication entre vous?

CARLOS ALVAREZ: Nous ne faisons pas de rapports concernant les usages malveillants. Ce n'est pas notre travail.

Nous analysons les données concernant les usages malveillants. Nous identifions les bureaux d'enregistrement qui pourraient être, qui pourraient enregistrer des grands nombres de domaines qui pourraient être considérés comme malveillants et nous partageons les informations avec l'équipe de conformité

pour qu'ils puissent aborder le processus au sein de leurs activités.

MICHAEL PALAGE: Merci.

BOBBY FLAIM: Mike, peut-être que vous pouvez en parler ensuite avec Carlos par la suite.

Bien. Il ne nous reste plus que quelques minutes. Donc, si vous voulez, nous allons fermer la queue ici. Kiran?

KIRAN MALANCHARUVIL: Je voudrais d'abord vous dire que je vous remercie pour cette session. Maintenant, je voudrais entendre ce que Mr Grogan a répondu au souci de Denise Michel de Facebook.

Et les enregistrements sont un problème. Nous avons soumis à l'ICANN un rapport qui contenait des milliers de noms de domaine qui avaient été enregistrés à point et on voyait que ces noms de domaine étaient, ressemblaient beaucoup à des noms de marque. Donc, j'aimerais beaucoup que Mr Grogan nous dise ce qu'il a à dire à propos des préoccupations que Denise a soulevées concernant la façon dont ce rapport avait été abordé.

ALLEN GROGAN: En général, nous ne parlons pas de cas individuels dans ce type de forums.

Deuxième point : je ne suis pas prêt à parler de cela. Je n'ai pas révisé ce dossier et c'est la partie de la conformité ici. Je ne suis pas vraiment aujourd'hui dans une situation, en situation de vous répondre.

KIRAN MALANCHARUVIL: Donc, vous n'avez jamais entendu parler de cela, des WHOIS frauduleux?

ALLEN GROBAN: Non. Vous m'avez demandé d'aborder ce que Denise a dit. Je ne suis pas prêt à le faire ici, parce que je n'ai pas étudié ce dossier. Je vous remercie.

KIRAN MALANCHARUVIL: Merci. Je remercie le panel pour cet intéressant [inaudible]. Je voudrais faire un commentaire à Denise. Vous parlez de noms de domaines qui étaient frauduleux.

D'abord, je voulais dire que je représente .industry. Le .industry a plus de cent bureaux d'enregistrement et des fois, nous devons prendre des actions dans les quarante-huit heures et ce

que je voudrais savoir, c'est pourquoi on n'écrit pas à ces registres du nom de domaine. Pourquoi il faut attendre deux mois avant de pouvoir mettre en place des mesures? Bien.

DENISE MICHEL: Nous contactons le bureau d'enregistrement directement, qui était responsable de l'enregistrement de ce domaine, pour essayer d'amener ce bureau d'enregistrement à respecter ses obligations dans le cadre du RAA et pour que ce domaine qui, selon nos informations, était – pour contrôler ce domaine. Donc, ensuite, on a parlé de cela au bureau de conformité de l'ICANN, puisque c'est leur responsabilité de s'occuper de ce type de plaintes contre des bureaux d'enregistrement qui ne respectent pas leurs obligations dans le cadre du RAA. Donc, c'est le processus. Il fonctionne comme ça et les obligations contractuelles sont telles que cela pour les bureaux d'enregistrement. Pour nous, c'est important de suivre la procédure et tout ce qui concerne les obligations exprimées par l'ICANN au niveau des contrats avec les bureaux d'enregistrement. Nous comprenons que le registre, comme je l'ai montré dans mes diapos, a aussi des responsabilités. Mais chez certains bureaux d'enregistrement, on constate que ce type de comportements est prévalent. Donc, nous pensions qu'il était important d'avoir ici un contrôle de ce processus et du temps que l'on mettait pour fermer ces deux domaines.

Bien. Je suis un petit peu… Je ne suis pas tout à fait d'accord avec vous, parce que vous dites que vous avez dû consulter la conformité de l'ICANN parce que les registres et les bureaux d'enregistrement… Les bureaux d'enregistrement qui ne prennent pas d'actions, vous auriez dû parler avec leur registre, ça aurait résolu le problème en une semaine. Ça aurait été plus rapide.

MICHELE NEYLON: Pour répondre à ce monsieur. Michele qui prend la parole, très brièvement. Je pense que Denise se plaint de noms de domaine .com si les registres n'ont pas les données WHOIS pour leur domaine. Peut-être que se plaindre au registre, si le registre continue à recevoir des plaintes va être en colère contre ce bureau d'enregistrement et va les renvoyer au bureau d'enregistrement. Mais pour .com ou .net, le bureau d'enregistrement est celui qui doit contrôler les données WHOIS et donc, si le bureau d'enregistrement a fait des changements… Je n'essaye pas de défendre ce bureau d'enregistrement. Il s'agit d'une relation. S'il s'agit d'un registre de type .org ou des TLD, je pense que la relation peut être différente, mais lorsque l'on parle des données WHOIS, elles doivent exister au niveau du bureau d'enregistrement.

Ce que j'essayais de dire, c'est qu'il y a un accord entre le registre et le bureau d'enregistrement. Si le registre, le bureau d'enregistrement ne prend pas d'actions, ne met pas en œuvre des actions, le registre peut le faire.

Si vous voulez, nous en parlerons plus tard.

BOBBY FLAIM: Nous avons encore quelques questions. Allez-y, monsieur.

PAUL MCGRADY: Les efforts… Pendant quinze ans, j'ai assisté à des choses un peu comme ce que Denise a décrit. Nous avions quelque chose de semblable qui arrivait. Nous pensions que c'était donc des informations semblables qui apparaissaient dans les plaintes UDRP. Nous avons écrit au bureau d'enregistrement qui n'était pas basé aux États-Unis. Nous avons suspendu le nom de domaine et pour pouvoir l'effacer, on nous a dit, l'ICANN nous a dit qu'une fois qu'un nom de domaine était suspendu, ce n'était plus un nom de domaine réel. Donc, c'était leur pratique générale. Bien. Donc, je pense qu'il faut contrôler tout cela et qu'il faut s'assurer que ces noms de domaine ont été suspendus, en tout cas si les choses fonctionnent comme ça.

Je pense qu'il y a peut-être une brèche ici que l'ICANN devrait corriger ou en tout cas essayer de voir comment cela peut être

résolu, parce que les gens nous disent, non, ce n'est pas nous, et à ce moment-là, c'est difficile comme situation. On a du mal à régler ce type de situation. Merci.

BOBBY FLAIM: Merci. Notre dernière question. Nick?

NICK SHOREY: Merci Bobby. Je voudrais dire… je pense que ça a été une discussion très intéressante d'abord. Donc, je remercie tous les intervenants de ce panel. Je crois qu'il y a eu des idées très intéressantes ici qui peuvent nous être utiles dans les mois à venir dans notre travail, pour voir comment nous pouvons améliorer la sécurité publique, les requêtes lorsqu'elles sont faites ou lorsque nous devons le faire comme Michele l'a expliqué. Il me semble qu'au sein de cette discussion, oui il faut qu'il y ait davantage de travail pour définir ce que nous voulons dire lorsqu'on parle d'usage malveillant et je pense que ça doit être fait. Ça sera une bonne chose.

Je pense aussi qu'il y a une distinction entre proactif et réactif et je dirais réponse proactive et réactive par rapport à ces usages malveillants. Donc, il faut voir pour la validation du WHOIS, il faut avoir une réponse, des actions proactives, et ensuite, il y a des réponses réactives. J'aimerais ici qu'on nous dise si un

registre voit son URL par exemple lorsqu'une demande de DNS est faite. Si l'on voit ces informations, qu'est-ce que ça lui donne au niveau de l'espace du cyber-délit. Ça donne beaucoup de données et s'il y a…

Je voudrais savoir… En tout cas, la prochaine fois, parce qu'il me semble que nous devons faire cela à nouveau, est-ce que nous pourrions avoir des opérateurs de compagnies d'hébergement? L'ICANN participe toujours à ce type de débats compliqués et donc, j'apprécierais que l'on ait un autre point de vue ici.

Donc, je pense qu'il serait bien de comprendre la collaboration qui existe et au niveau des opérateurs de réseau, de l'hébergement, pour avoir une idée plus large au sein de ce même débat. Merci beaucoup.

BOBBY FLAIM: Merci. Je crois que c'est une très bonne idée de demander à des fournisseurs d'hébergement de venir donner leur opinion. Michele.

MICHELE NEYLON: Moi aussi, je suis un bureau d'enregistrement, un fournisseur d'hébergement, etc.

Donc, en termes de demande de DNS pour l'URL, je pense qu'il faut qu'on vous expliquer un petit peu plus comment le DNS fonctionne. Le registre ne va pas voir cela. Le registre va savoir quels serveurs de noms utilisent un nom de domaine, mais il ne va pas voir toutes les demandes, les requêtes de DNS pour un nom de domaine dans un registre. Il va voir les autres niveaux. Mais en tout cas, quand vous avez besoin d'aide, je serais ravi de vous aider et vous pouvez compter sur moi.

CARLOS ALVAREZ: Carlos de l'ICANN. Je voudrais ajouter ici un petit point puisque c'est l'heure. Mais je dirais qu'il y a environ 2 000 bureaux d'enregistrement que nous avons décidé d'analyser de près. En ce qui concerne l'usage malveillant, l'hameçonnage et les zombies – ça il y en a moins.

Donc la communauté de sécurité concernant les bureaux d'enregistrement que les gens peuvent accuser d'enregistrer des noms de domaine qui utilisent des pourriels, cela ne rentre pas dans l'action de l'ICANN. Le GAC a fourni un avis en 2013.

On ne mentionne pas ce type de choses. Nous ne pouvons pas aborder ce type de problèmes. Nous ne pouvons pas travaillé avec ces bureaux d'enregistrement. Si nous faisons une révision d'un bureau d'enregistrement, nous passons cela au bureau des conformités et la conformité va faire son travail. Donc, ce que je

veux dire ici, c'est que c'est la communauté qui doit aborder ce type de problèmes si la communauté pense qu'il faut aborder ce type de problèmes. Mais la communauté doit s'occuper de ce problème, doit en parler du point de vue de la sécurité, parce que ce n'est plus disons dans le cadre de nos fonctions.

ALLEN GROGAN: Rapidement, je voudrais que ce soit clair que les noms de domaine qui ont été suspendus suite à des rapports d'usage malveillant vont rester suspendus pendant les deux mois suivants cette plainte.

GIOVANNI SEPPIA: Merci Bobby. Je pense que la discussion d'aujourd'hui a été très intéressante. C'est important d'avoir une éducation, une coopération et un dialogue entre toutes les parties prenantes. Lorsqu'on parle d'usage malveillant, il ne s'agit pas de montrer du doigt des parties qui sont concernées. Il s'agit ici de bien comprendre et de bien voir ce que nous pouvons faire tous ensemble.

DENISE MICHEL: Eh bien, c'est important de comprendre que lorsqu'un nom de domaine est utilisé pour attaquer des utilisateurs Internet, c'est ça la fraude. Si ce nom de domaine se sert des informations de

ma société, il ne devrait plus être utilisé et il devrait être mis en suspension.

Si Blacknight, la société de Michele, est mon bureau d'enregistrement. Je sais qu'ils vont prendre des actions là-dessus. C'est ce qui serait fait s'ils avaient été mon bureau d'enregistrement. Ils fournissent un service qui nous permet de mettre en suspension ces noms de domaine dans les vingt-quatre heures. Ce n'était pas le cas.

Et la suspension n'est pas une résolution ici. On a beaucoup de défis à relever dans ce domaine et ce que je tiens à souligner est le fait que je suis très contente que l'équipe de conformité commence à travailler et que ce soit une équipe importante pour le nouveau PDG. Merci.

ALICE MUNYUA: Merci. Je voudrais remercier les membres du panel de leur présentation et d'avoir respecté les délais qui leur avaient été assignés. Je vous remercie tous des questions que vous avez posées, je sais que vous en aviez d'autres. Les membres du panel avaient des présentations bien plus détaillées. Donc, si vous être intéressé par les détails de certains des sujets qui ont été présentés aujourd'hui, nous aurons les présentations publiées en ligne.

Je remercie Bobby qui a modéré la séance et Vivianne qui l'a organisée.

Nous allons maintenant passer à la séance suivante concernant la sécurité publique sur le WHOIS. Merci.

[Applaudissements].

[FIN DE LA TRANSCRIPTION]