ICANN79 | Forum de la communauté – Séance plénière At-Large organisée par NARALO
Mardi 5 mars 2024 – 4h15 à 5h30 SJU

MICHELLE DESMYTER : Cette séance va commencer, veuillez lancer l'enregistrement. Merci.

Bonjour et bienvenue à cette table ronde de NARALO. Je suis Michelle DeSmyter et je suis responsable de cette séance. Veuillez noter que cette séance est enregistrée et qu'elle dépend des normes de comportement de l'ICANN.

Au cours de cette séance, les questions et les commentaires seront lus à voix haute que s'ils sont soumis dans la partie du Zoom des questions et des réponses. Si vous souhaitez prendre la parole pendant cette séance, levez la main sur Zoom, nous vous donnerons la parole et vous pourrez allumer votre micro sur Zoom. Les personnes qui sont sur place pourront prendre un micro et prendre la parole.

Cette séance comprend un service d'interprétation en anglais, en espagnol, en français. Donnez votre nom et dites la langue dans laquelle vous allez parler si vous ne parlez pas l'anglais. Veuillez parler à une vitesse raisonnable.

Je vais maintenant donner la parole à Greg Shatan, président de NARALO.

GREG SHATAN : Bonjour à tous, bienvenue à cette table ronde de NARALO. Beaucoup d'entre vous le savent, il s'agit d'une tradition pour At-Large. La RALO qui reçoit la réunion dans sa région va organiser ce type de discussions et c'est le cas aujourd'hui. Nous allons discuter de questions qui nous intéressent tous beaucoup. Tous ceux qui étaient un peu à l'origine de l'Internet le savent, on parle beaucoup actuellement d'utilisation malveillante du DNS et nous avons aujourd'hui des membres de l'ICANN qui nous accompagnent pour ce panel.

J'ai Laureen Kapin, assistante-directrice pour la protection du consommateur international et elle à la Commission fédérale du commerce des États-Unis et elle est présidente sortante du groupe de travail de sécurité publique du GAC. Je la félicite pour le travail qu'elle a réalisé lorsqu'il est à ce poste. Nous avons aussi à côté de moi et Graeme Bunton, directeur exécutif de l'Institut d'utilisation malveillante du DNS du Canada. À côté de moi, Steve Crocker, il n'est pas nécessaire de le présenter. Vous le connaissez, vous en avez entendu parler et c'est un honneur pour nous de le recevoir. Aujourd'hui, dans ce panel, c'est une bonne chose de savoir qu'il va travailler avec nous sur la question du DNS et de l'utilisation malveillante du DNS. Nous savons qu'il possède énormément de connaissances dans ce domaine. Steve est le président de l'Institut de recherche de Edgemoor. À côté de lui, nous avons Ram Mohan qui porte différentes casquettes et il est actuellement directeur stratégique à Identity Digital et nous sommes heureux qu'il soit aujourd'hui avec nous. Ensuite nous avons Reg Levy. Vous pouvez venir ici à nos côtés, je vais l'obliger à déménager. C'est la directrice de la conformité de

Tucows et c'est quelqu'un qui est là parmi nous à l'ICANN depuis de nombreuses années.

Nous sommes très heureux de compter sur ce panel qui va nous parler de l'utilisation malveillante du DNS et des domaines dans l'économie numérique. Il s'agit d'un panel qui va parler du point de vue de l'utilisateur final et la perspective de l'utilisateur final va être prise en compte dans cette conversation.

Il y a eu beaucoup de conversations lors de cette réunion de l'ICANN sur l'utilisation malveillante du DNS avec, différentes nouveautés, le RDRS par exemple, ce qu'on appelle aussi l'amendement de l'utilisation malveillante du DNS et avec les parties contractantes. Et nous avons toute une variété de problèmes avec différentes définitions de ce qui est l'utilisation malveillante du DNS. On en a déjà beaucoup parlé, ce n'est plus nécessaire de définir l'utilisation malveillante du DNS.

Nous allons commencer par donner la parole à Graeme Bunton en tant que directeur exécutif de l'Institut d'utilisation malveillante du DNS. Toute sa vie a été consacrée à ce thème. Nous allons écouter son opinion à ce propos.

GRAEME BUNTON : Merci Greg. Je pense qu'ici le point important, peut-être que l'on peut commencer par parler de ces amendements que vous avez mentionnés qui vont être mis en œuvre à partir du 5 avril et qui vont donner lieu à des obligations claires pour les bureaux d'enregistrement et les opérateurs de registre pour les enregistrements concernant les

enregistrements malveillants avec une série d'outils à appliquer dans ce sens.

Je pense que le futur nous encourage un peu. On a une vision positive du futur vu ces nouveaux outils, et je pense que ces outils vont être utilisés bientôt, une fois que cet amendement sera appliqué. Je crois que cela va changer vraiment le paysage, l'environnement concernant l'utilisation malveillante du DNS, un changement que nous allons suivre de près. Cela va donner lieu à des travaux de la communauté, cela va changer la façon dont l'Internet fonctionne aussi, je pense.

Nous n'allons pas résoudre le cyberdélit. Nous n'allons pas empêcher certains de faire des choses interdites sur le DNS, mais on va commencer à contrôler un peu plus les choses, de quelle manière cela va changer l'activité de ces mauvais acteurs. Est-ce qu'ils vont passer à d'autres types de sites Internet ? Est-ce qu'ils vont passer à des sous-domaines qui ne dépendent plus de l'ICANN ? Est-ce qu'ils vont passer par des chemins alternatifs ? Nous le verrons, c'est quelque chose à suivre de près. Je voulais vous faire part un peu de mon opinion. En tout cas, je pense que c'est un changement tout à fait positif qui va avoir lieu dans notre communauté.

GREG SHATAN : Merci Graeme. Je crois que c'est un bon début. Je suis navré de savoir qu'on ne va pas résoudre le cyberdélit, mais les méchants avancent toujours et les gentils doivent continuer à lutter contre ces méchants.

À propos justement de ceux qui sont honnêtes et qui travaillent dans le domaine de la conformité, nous allons donner la parole à Laureen

Kapin. Je pense que Laureen a des diapositives. Nous allons lui donner la parole.

LAUREEN KAPIN : Je suis Laureen Kapin. Je vais vous parler en tant que coprésidente du groupe de travail de sécurité publique et je suis aussi directrice assistante pour la commission de protection du consommateur. Je dois dire que je parle en mon nom, c'est important. Ici, vous avez un petit post-it qui indique cela.

Je voulais partager avec vous un peu une perspective du monde réel tel qu'il est, comment certains types d'utilisation malveillante du DNS peuvent exister et peuvent apparaître comme une fraude dans le monde réel. Je vais vous présenter des statistiques, je vais vous présenter FTC de 2023 avec les statistiques de cette année-là pour vous donner un peu de contexte et pour une question de clarté. Ces statistiques ne correspondent pas aux statistiques d'utilisation malveillante du DNS qui ont une définition très spécifique dans notre monde de l'ICANN.

Ici, ce sont des statistiques de fraude générale que la commission a collectées puisque nous sommes l'organisme qui lutte contre ce type de délits. Nous collectons des millions de plaintes dans tous les États-Unis au niveau des forces de l'ordre, au niveau des plaintes de consommateurs, des victimes et des agences de protection des consommateurs. Nous travaillons même avec des organisations des forces de l'ordre qui sont dans le monde entier. Nous avons vraiment

beaucoup de données. Cela nous donne beaucoup de données que nous pouvons partager avec le public.

Parlons un petit peu de notre nom. On parle de Commission fédérale du commerce. Ici on parle de commerce dans le sens des transactions commerciales. On ne parle pas de tarifs douaniers ou d'exportation. Prochaine diapositive.

Voilà les statistiques dont je vous parle qui vous donnent une perspective au niveau du monde entier concernant l'utilisation malveillante du DNS contre les utilisateurs, vous et nous qui utilisons l'Internet. Je dirais de manière générale que ces plaintes concernant les fraudes augmentent. On a reçu 2,6 millions de plaintes concernant ces fraudes. Ici, vous voyez ce à quoi cela correspond en milliards de dollars. Les personnes souffrent vraiment de graves pertes quand elles sont victimes de ce type de fraude.

En termes d'imposture, c'est une série de catégories avec des impostures au niveau des entreprises, au niveau des gouvernements. On sait qu'un des thèmes dont on parle beaucoup à l'ICANN, ce sont les domaines qui prétendent être des business légitimes ou des entreprises légitimes et qui ne le sont pas. C'est une catégorie de fraude.

Et en termes de méthodes de contact, un des systèmes préférés de ces fraudes est l'e-mail, la méthode de contact par e-mail. C'est une méthode qui est très utilisée et aussi très analysée dans le domaine de l'ICANN par la communauté.

Maintenant, en termes de pertes, une des choses que nous avons aussi comprises à travers ces statistiques, c'est que les gens perdent aussi de

l'argent à cause de fraudes liées à des investissements. Ce type de fraude concerne par exemple les cryptomonnaies qui deviennent de plus en plus répandues. On a ici le deuxième niveau de fraude en somme d'argent. À nouveau, ici ces fraudes basées sur une imposture qui augmentent avec les achats en ligne, les jeux, la loterie, le tirage au sort, etc. les investissements et autres.

Voici les méthodes de contact. Comme je l'ai dit, les e-mails sont les plus répandus, mais on a aussi les appels téléphoniques et les SMS. Ceux qui se sont traduits par les plus fortes pertes, c'est au premier rang les réseaux sociaux. Ce qui est très fréquent pour l'ICANN, c'est les pubs en ligne, les pop-ups, les pubs intempestives, et ensuite les sites Web et les applis.

Maintenant, parlons d'hameçonnage. Un des types d'utilisation malveillante de DNS sur lesquels nous concentrons nos données, sur les 12 derniers mois jusqu'à la date du 2 mars 2024, nous avons reçu plus 1 000 rapports, 100 au cours du mois écoulé, ce sont des plaintes concernant l'hameçonnage, et ces rapports pour ce qui est des montants payés en raison d'arnaques d'hameçonnage s'élèvent à 2,2 millions. Encore une fois, le premier produit ou service auquel ceci est rattaché, ce sont de fausses entreprises ou des imposteurs dans le domaine de l'entreprise.

Je m'arrête là pour ce qui est des données. On va avancer jusqu'à la dernière diapositive, juste pour que vous le sachiez. Si vous voulez en savoir davantage sur ces données de la commission du commerce des États-Unis, nous avons notre livre de données ainsi que nos données en accès libre public. Vous pouvez comparer les plaintes, les tendances

d'une année à l'autre, d'un trimestre à l'autre, vous pouvez voir les tranches d'âge les plus susceptibles d'être arnaquées, ceux qui payent le plus. Vous pouvez comparer les méthodes de contact et vous pouvez analyser cela de tous les angles, de toutes les perspectives en temps réel. C'est une ressource franchement richissime.

Maintenant, je vous donne ces indications parce que ce que je veux souligner clairement, c'est que souvent, on se perd dans des débats, on se dit « Comment est-ce qu'on devrait définir cela ? Vers qui doit-on se tourner ? » Certes, ce sont des questions qui ont leur importance aussi, mais je pense aussi qu'il faut tenir compte de l'effet que ça a sur l'utilisateur final, c'est-à-dire la véritable victime ici. Ce sont des personnes qui ont été lésées dans beaucoup de cas et à qui on a enlevé leurs économies de toute leur vie, leur retraite. Parfois, ils perdent leur maison, parfois ont même sacrifié leur vie parce qu'ils étaient complètement dépassés. Cela peut sembler dramatique, mais je le dis sans exagération. Les conséquences peuvent aller vraiment de 0 à 100. On peut passer de quelqu'un qui sait que c'est une arnaque et qui tourne la page, ou quelqu'un qui est véritablement au fond du trou. Il faut le garder à l'esprit.

Voilà, je m'arrête ici.

GREG SHATAN : Merci. Ces statistiques donnent à réfléchir, aucun doute.

Maintenant, je me tourne vers Ram Mohan, celui qui porte le nom de la mémoire of informatique, la Ram. Ram, qu'est-ce que vous en pensez ?

On a une définition très étroite de cette utilisation mal du DNS, mais quand même, qu'est-ce que vous pouvez en dire ?

RAM MOHAN : J'aime le concret, parlons de ce qui a été fait.

Il faut parler du taux de prévalence et de l'atténuation de ces utilisations malveillantes. À mon sens, c'est le critère le plus parlant. Prenons l'hameçonnage qui est un véritable fléau qui n'épargne personne dans notre quotidien. Il y a une différence dans les conséquences. On peut démanteler ou surveiller une campagne d'hameçonnage. La différence entre le démantèlement au cours des six premières heures, c'est-à-dire dans les six heures après l'avoir découvert et 18 heures, on a une petite différence de 12 heures, cela change absolument tout.

Avec ce genre de choses, les conséquences sont absolument concrètes et tangibles. Il n'y a pas que la fréquence, le nombre de fois que cela s'est reproduit, il n'y a pas que le volume ou le temps nécessaire pour le démanteler. En tant qu'industrie, en tant que groupe communautaire, on doit regarder le temps médian, le temps moyen en quelque sorte. Et on doit sans relâche s'attacher à démanteler cet hameçonnage. Malheureusement, dans le monde ICANN, on s'attaque souvent aux bureaux d'enregistrement, aux opérateurs, on dit : « Vous devriez en faire un peu plus, etc. » Mais il y a le revers de la médaille aussi. L'utilisation malveillante du DNS passe souvent par le contexte. On peut croire déceler une utilisation malveillante d'un certain angle, mais en fait, quand on regarde le contexte, ce n'est pas le cas.

On a certains algorithmes, par exemple, qui ont analysé des phrases, des phrases qui pourraient s'apparenter à un discours de haine ou des phrases qui pourraient inciter au crime. Le résultat, c'est que parfois des travaux universitaires sont effacés ou annulés et parfois, certains se font piéger. C'est le contexte.

Quand vous regardez les utilisations malveillantes, le contexte est tout aussi important que le contenu. J'irai jusque-là. Dans cet écosystème, on estime que les parties contractantes sont celles qui doivent influencer de manière positive ces utilisations malveillantes, réduire ces utilisations malveillantes et augmenter le niveau de sécurité sur Internet. Mais il y a tout un autre lot d'acteurs sur le terrain et il faut miser sur eux, comprendre ce qu'ils font. On a les compagnies hôtes, les entreprises hôtes, d'autres fournisseurs également. Je sens maintenant tout ce qui lui et parfois, vous verrez que quelque chose qui ressemble drôlement à une utilisation malveillante, ensuite une communication est établie, disons que la requête vient arrive sur la table de l'ICANN, l'ICANN va voir le registre. Le registre dit : « Allez voir le bureau d'enregistrement » et le bureau nous dit : « Écoutez, allez plutôt au fournisseur de services hôte d'Internet parce que c'est en fait une question qui relève du contenu. » Et les gens se passent la balle comme cela. Il faudrait trouver un moyen de les inviter dans le processus de recherche de solutions. À la base de l'ICANN, ces fournisseurs sont souvent écartés de la table de discussion. Beaucoup d'entre eux agissent noblement, mais ces bonnes pratiques ne sont souvent pas incorporées à notre travail.

Dernier point, comme Graeme l'a bien dit, le but n'est pas d'empêcher, le but est d'atténuer, de réduire. Et deuxièmement, au sein de notre propre écosystème, s'il y a des choses claires et nettes que nous pouvons faire pour répondre plus rapidement et pour couper court aux mauvais comportements dès le départ, nous devons le faire.

Dans notre propre registre, on a un programme d'essai. On ne l'a pas fait dans un environnement de production, mais on teste un programme qui permettra, au moment de l'enregistrement d'un nom de domaine… Et dans certains cas d'ailleurs, le registre connaît le titulaire du nom de domaine. Souvent à 60 %, 70 % 80 % du temps, c'est caché derrière un nom fiduciaire. Il n'est parfois pas si difficile de trouver qui fait la demande.

Vous savez, les malfaiteurs sont paresseux parfois quand ils trouvent un mécanisme qui marche. Ils finissent par mettre les bouchées doubles. Et nous sommes responsables. Nous devons nous doter de programmes capables d'identifier ce genre de schéma de paresse. Et c'est là qu'on peut resserrer l'étau.

On a lancé un programme d'essai au sein de notre propre entreprise où, au moment de l'enregistrement, si on remarque qu'il y a la possibilité qu'un groupe de noms ou qu'un nom en processus d'enregistrement a l'intention ou en tout cas laisse entrevoir un comportement déjà vu de la part d'un acteur malveillant, on met ces noms sur une liste de suspects à surveiller. Quand ces gens sont identifiés comme étant malveillants, on cherche à les démanteler, à annuler leur activité en une heure au lieu de prendre six ou sept heures comme c'est le cas maintenant. Comme j'ai dit, l'effet est beaucoup plus fort quand on

arrive à agir très vite si vraiment les gens sont des criminels qui essaient de les enregistrer.

Je me concentre sur des choses pratiques qui peuvent être faites et je milite aussi pour l'intégration de ceux qui sont encore exclus de la table des négociations de l'ICANN à notre discussion. Merci.

GREG SHATAN : Merci Ram. Il y a beaucoup de choses à décortiquer ici. On a déjà parlé justement de l'intégration de certaines de ces parties à notre table de discussion, mais ces derniers sont absents aujourd'hui. J'espère que cela va changer.

Je me tourne maintenant vers Steve Crocker, PDG de ERI. Je pense qu'il a beaucoup de choses à dire en transition. Et même si ça n'a rien à voir avec les propos de RAM, ce sera intéressant, nul n'en doute.

STEVE CROCKER : On va afficher les diapositives. En attendant, je vous dirais que j'ai travaillé dans un domaine qui est proche du problème de l'utilisation malveillante du DNS et il y a des chevauchements et vous les verrez. J'ai travaillé dans un domaine qui s'appelle tout ce qui concerne le WHOIS, l'accès aux données d'enregistrement et cette collecte de données d'enregistrement, comment elle devrait être gérée, comment y accéder. C'est ce que nous appelons le projet Jake, puisque Jake était la personne qui était à l'origine du système WHOIS.

Je vais introduire la question. J'ai analysé pendant une période que l'on peut évaluer en décennies, j'ai essayé à plusieurs reprises de voir

comment on pourrait collecter toutes ces données d'enregistrement. Lorsque j'ai quitté le Conseil d'Administration en 2017, je n'avais pas encore pu mettre en place un système qui pourrait permettre à tout le monde de collaborer sur ces questions et de réfléchir à cela et de mettre en place une série d'idées.

Nous avons travaillé pour réaliser ce projet. En même temps, j'ai participé aux discussions internes sur le processus d'élaboration de politiques de la phase 1, de la phase 2, le PDP accéléré, tout ce qui était lié aux services de demande de données d'enregistrement. Ce qui peut paraître ici comme un résultat positif serait que l'objectif serait d'avoir un système qui permettrait de garantir la protection de la vie privée et l'efficacité de ce système.

La protection de la vie privée, l'efficacité et l'exactitude. Est-ce qu'on peut avoir les trois ? Je dirais que oui, c'est possible. Il y a des travaux qui ont été faits qui montrent que cela est possible. Il y a eu une série de discussions sur certaines questions qui étaient assez simples et il y a des points qui n'ont pas été abordés.

Qu'est-ce que le RGPD ? Le RGPD est arrivé et a un peu pris la place de beaucoup de choses et a changé beaucoup de détails concernant les structures qui concernaient la protection de la vie privée. Cela nous a menés à des changements. Nous avons dû regarder tout cela à nouveau. Je ne rentrerai pas trop dans le détail de cette diapositive. Je peux mettre ces diapositives à votre disposition si elles vous intéressent.

Voilà un diagramme de ce qui est l'enregistrement de noms de domaines. C'est assez simplifié. Nous avons les opérateurs de registre en haut, en dessous les bureaux d'enregistrement, les bases de données associées. Ici, nous avons une relation avec le titulaire de nom de domaine à droite et à gauche, les personnes qui vont demander ces données. C'est un diagramme avant le RGPD.

Ici, le WHOIS historique. Il y avait 5 milliards de demandes avant que le système soit adapté au RGPD. Et maintenant, il y a des demandes pour informations publiques, informations non publiques. Nous avons des chiffres qui sont tout à fait différents et qui posent justement la question de ce qu'étaient ces demandes auparavant. Il y a une série de réponses à ce propos et j'ai personnellement du mal à comprendre cet ordre de magnitude dans lequel nous nous trouvons actuellement.

Nous avons préparé un modèle global. Ensuite, nous avons travaillé sur les questions liées à l'exactitude, à la protection de la vie privée et autres. Et nous avons constaté que lorsque l'on parlait de ce que devaient être ces règles, chacun avait une opinion et avec des règles parfois qui existait aussi. Un opérateur de registre avait des règles, un bureau d'enregistrement avait ses règles, certains gouvernements avaient leurs règles. Tout cela doit devenir plus explicite et être documenté d'une manière ou d'une autre. Quand on analyse la situation, on se rend compte qu'un bureau d'enregistrement peut avoir certains désirs concernant la façon dont il veut que cela fonctionne, mais tout doit dépendre de politique. Il n'y a pas de priorités concernant la pertinence de tout cela. Un bureau d'enregistrement peut essayer de satisfaire les règles de l'Union européenne, les règles

qui existent aux États-Unis, mais il va constater qu'il y a certaines instances qui ne peuvent pas être satisfaites. On a pensé qu'il y avait un document qui devait exister concernant ces règles, non pas ce qu'elles devaient être, mais un document concernant ce qu'elles étaient et leurs objectifs, comparer ces règles en fonction de la région dans laquelle elles étaient appliquées pour voir s'il y avait une pertinence entre elles.

Au niveau des demandes, qui sélectionne quelles données et dans quelles circonstances ? Comme je l'ai dit, ce n'est pas encore le moment ni l'endroit de rentrer dans le détail. Nous avons travaillé avec Laureen et avec Graeme dans ce groupe de travail et nous voulions savoir quel type de demandes on pouvait faire, dans quelles circonstances, obtenir ici une des précisions. Nous avons ici un modèle de demandes. Nous allons passer cela rapidement.

Ici, vous voyez un point très important parce que nous sommes dans un domaine dans lequel on nous dit que chaque demande de données non publiques doit être examinée, évaluée en fonction de son contexte, de la légitimité de son objectif. Il faut qu'il y ait un avocat qualifié aussi qui entre en jeu ici parce que cela doit être évalué. À ce moment-là, on peut se demander quelles sont les données qui nous permettent de prendre cette décision, quel type de données ont été collectées dans le système. On ne peut pas demander cela à un titulaire de nom de domaine en temps réel pour répondre à ces questions.

Je pense que quelles que soient les demandes qui vont être faites et les décisions qui seront prises, on devrait parvenir à une routine avec des organisations qui travaillent de manière raisonnable. Cela va permettre de réduire les coûts, le temps de travail et on va augmenter la

cohérence et la transparence de ce système. On va passer d'un système datant du 19ème siècle à un système datant du 21ème siècle, ce qui est très important.

Cela va impliquer qu'il faudra voir quelles sont les règles du jeu qui sont appliquées, par exemple un avocat qui va travailler sur la propriété intellectuelle va vous dire : « Si vous faites une demande au nom de votre client, vous allez devoir nous indiquer la relation, le problème. Et s'il y a un mensonge, nous saurons où vous trouver en cas de mensonges. Nous pouvons faire un audit de votre demande. » Quand on parle au bureau d'enregistrement par exemple, on peut avancer un petit peu plus vite pour que les choses puissent avancer à un rythme plus rapide. Il y a différents types d'accords de ce type. Ici, c'est un peu ce que je disais, c'est-à-dire certaines vérifications qui peuvent être réalisées de manière automatique, mais revenons un peu à la situation de l'utilisation malveillante du DNS.

Beaucoup de transactions de ce type ont beaucoup de choses en commun au niveau de leur manière d'agir concernant le DNS, l'utilisation malveillante du DNS. Il y a une série de systèmes partagés qui sont communs ici, et c'est une des conclusions à laquelle je suis arrivée en analysant toutes ces utilisations malveillantes.

GREG SHATAN : Vous parlez du temps permettant d'atténuer les problèmes, c'est un aspect important de tout cela. Et il me semble me souvenir que vous souhaitiez que l'on mette en place une machine pour remplacer le WHIS. Steve, vous nous avez parlé de la situation des bureaux

d'enregistrement. Je voudrais maintenant donner la parole à Reg de Tucows qui va prendre la parole.

REG LEVY : Merci. Je vous remercie aussi de m'avoir permis de prendre la parole en dernier. J'apprécie beaucoup les indications de Ram indiquant qu'il faut agir rapidement parce qu'il y a des domaines qui vont être détournés. Je dirais que 50 % des situations d'utilisation malveillante sont des utilisations malveillantes ou du détournement. C'est quelque chose qu'il faut voir directement avec le revendeur et le titulaire de nom de domaine de façon à pouvoir faire des changements.

Comment faire cela ? D'abord, il y a toute une série de questions qui entrent en jeu. Est-ce qu'ils vont nous croire ? Il y a toute une série de choses. Nous allons suspendre un domaine en général, nous commençons par cela. C'est la première action. Et Tucows, de manière interne et en partenariat avec d'autres revendeurs et personnes qui travaillent dans ce domaine, nous regardons les tendances. Il y a eu toute une série de discussions concernant les données des titulaires. Très souvent, cela est corrélé à une adresse IP. Les malfaiteurs, très souvent, nous allons les contacter. Parfois, on constate qu'ils enregistrent un domaine chez nous et chez d'autres opérateurs. Ils travaillent avec des données volées, ils enregistrent des noms de personne, ce sont des vols d'identité de ces personnes. Les informations liées à l'adresse IP représentent une bonne indication d'une attaque malveillante qui est en cours, parce qu'on a un contenu malveillant qui a été enregistré.

Nous travaillons de manière interne et externe. Nous avons plusieurs fournisseurs de services Internet avec lesquels nous travaillons. Nous travaillons de manière synchronisée avec les informations de l'adresse IP. Prenons un autre bureau d'enregistrement : « Nous avons constaté une attaque sur notre réseau et voilà quelques données qui ont été enregistrées et qui sont liées à un nom de domaines qui a été enregistré dans votre système. Voyons quelles sont les actions que l'on pourrait mettre en œuvre pour répondre à cela. »

Nous avons conclu qu'il n'y a pas de recoupement entre les données d'enregistrement et les utilisations malveillantes de DNS. Une des questions qu'on nous a posées, c'est la suivante comment : est-ce que RDRS peut faire diminuer les utilisations malveillantes ? Le RDRS est censé donner des informations au Conseil concernant la popularité d'un système de requêtes centralisé. Mais c'est complètement en dehors du ressort du RDRS. Et le genre de requêtes qu'on reçoit par le biais du RDRS en général n'ont rien à voir avec l'utilisation malveillante des DNS. C'est plutôt lié au contenu malveillant, ce qui est une question complètement externe à cette conversation. Ce n'est pas du tout dans notre périmètre.

J'ai encore d'autres petites notes ici. Steve a dit qu'il faudrait que les demandeurs indiquent exactement ce qu'ils veulent pour que ce soit fourni dans un format uniforme et c'est ce que le RDRS a fait. Ce n'est pas lié aux utilisations malveillantes du DNS. Et avec toutes les informations nécessaires, nous pourrons réviser chaque cas différemment. C'est ce qui est nécessaire.

En tant qu'avocate, je me spécialise en propriété intellectuelle, mais cela ne suffit pas pour avoir accès à toute la base de données. Non, c'est un argument irrecevable. Le fait que quelqu'un ait un titre quelconque ne veut pas dire que cette personne aura forcément le droit ou l'accès à des données WHOIS sur un nom de domaine spécifique. Non, ce n'est pas le cas. Je m'égare un peu. On parle d'ici d'utilisation malveillante des DNS. C'est complètement différent des données WHOIS. Il faut bien faire le départ entre ces deux-là.

Le .cn présente une des politiques de données d'enregistrement les plus strictes de toute l'industrie et affiche des niveaux d'utilisation malveillante très élevés. Alors que .com, c'est très élevé également parce que c'est .com, tout le monde le veut ; voilà pourquoi il y a autant d'utilisation malveillante. Si j'envoyais un lien tout à fait légitime à tucows.link, tout le monde croira que c'est faux. C'est pour ça que .com a autant d'utilisation malveillante parce que c'est celui que tout le monde veut et il est très convoité.

J'ai vu que Steve a indiqué que la protection des données privées était très importante dans notre écosystème et je suis très contente d'entendre ça. Comme Laureen l'a dit, il y a beaucoup de fraudes sur l'Internet et le plus clair de cette fraude vient du fait que ces informations étaient publiques autrefois. C'est une excellente source d'information gratuite sur les gens, les adresses e-mail, les numéros de téléphone, les adresses des domiciles, etc. Tout cela était utilisé pour perpétrer des utilisations malveillantes contre des titulaires de noms de domaine qui sont en fait des utilisateurs finaux d'autres produits et ces gens-là méritent une protection.

Encore une fois, le paysage des utilisations malveillantes du DNS n'a pas changé. Cela n'a pas aidé mon équipe à démanteler ces malveillances. Ce sont deux questions complètement différentes.

GREG SHATAN : Merci Reg. Cela fait réfléchir. Vous avez le privilège de passer la dernière.

Je veux maintenant permettre à qui veut bien parler de répondre, peu importe qui dans le panel. Vous pouvez aussi enrichir la conversation. Mais si vous n'avez pas de questions ou de commentaires, je vais regarder les questions qu'il y a en ligne. Mais tout d'abord, Laureen a levé la main.

LAUREEN KAPIN : Je vous ai aligné beaucoup de statistiques décourageantes tout à l'heure, mais je vais essayer de rétablir l'équilibre ici en vous remerciant et en répondant à certains des points soulevés tout de suite.

Je crois que les amendements quant à l'utilisation malveillante du DNS sont une excellente nouvelle. Cela a été lancé par les parties contractantes à l'ICANN. C'est une initiative proactive qui donne à la section conformité les outils pour se mesurer et triompher des acteurs malveillants.

D'autres bonnes nouvelles, ce sont les autres mesures et les rapports qu'on reçoit de l'institut de l'utilisation malveillante du DNS. Cela peut beaucoup nous aider et peut aiguiller les politiques futures. Je pense que l'organisation ICANN avance aussi avec son système Metrica et va commencer à le mettre en opération. C'est une bonne chose. Je pense

que cela nous donnerait des informations plus précises au niveau des bureaux d'enregistrement et des opérateurs de registre. Je suis contente de voir le travail proactif que les registres et que les bureaux d'enregistrement effectuent pour essayer de détecter le plus vite possible les mauvais acteurs, les mauvais éléments dès le début plutôt que de simplement réagir à une plainte. Ce travail est d'une importance incommensurable et pourrait servir de modèle de pratiques optimales qui permettra à la communauté d'être énergique, d'être enthousiaste dans ces efforts d'anticipation, plutôt que de réagir tout le temps à une mauvaise situation ou pire encore une crise. Voilà ce que je voulais dire.

GREG SHATAN : Merci Laureen.

Reg, je vous ai vu lever la main. Je vais répondre à l'idée voulant qu'il n'y a aucun lien entre les utilisations malveillantes du DNS et les données sur les titulaires des noms de domaine. On parle de mauvais agissements et mauvais acteurs. L'utilisation malveillante, c'est un mauvais agissement. Il n'y a pas de lien entre les données WHOIS et les données RDRS et le mauvais agissement. Mais quand on cherche le mauvais acteur coupable de ce mauvais agissement, les données WHOIS ou d'autres données ou d'autres choses comme des adresses IP, on peut retracer le crime, cela va nous mener vers le mauvais acteur. Et pour couper court à ces mauvais agissements, on essaie d'identifier les mauvais acteurs, certes, on essaie aussi de couper leurs approvisionnements et leurs armes à leur disposition. Voilà ce que j'avais dit, ce que j'avais à dire là-dessus.

À Graeme et ensuite à Steve.

REG LEVY : Merci. C'est ce que je voulais dire pendant mon introduction. Des amendements sont censés donner à l'ICANN les outils nécessaires afin d'arrêter les mauvais acteurs, c'est-à-dire les bureaux et les opérateurs qui soutiennent et qui profitent des utilisations malveillantes de DNS et qui profitent de leur inaction. Des collègues de Tucows entre autres travaillent sans relâche pour mettre en place ces garde-fous et nous avons hâte de voir les changements à venir parce que l'ICANN a bien signalé certains cas. Nous espérons que cela va déboucher. C'est ce que la communauté fait, c'est ce que les parties contractantes font également. Et nous avons bien hâte de voir les données qui découleront de ces amendements afin qu'ensuite nous sachions les étapes suivantes.

Il y aura d'autres étapes sur notre chemin. Quelqu'un l'a dit, les malfaiteurs sont toujours un petit pas derrière nous. C'est bien de toujours anticiper. C'est un outil qu'on a. On a bien hâte de voir les données qui en ressortiront parce que c'est très utile. Nous attendons avec intérêt ce rapport et ce dénouement. Il sera intéressant de connaître l'étape suivante.

GREG SHATAN : Merci Reg. Vous et Graeme ont parlé de la section conformité de l'ICANN. C'est bien dommage que je n'ai personne de cette section ici avec nous dans le panel, parce que c'est la variable principale ici. On a maintenant l'armure, on a l'arsenal. La question suivante se pose : est-

ce qu'ils ont la niaque pour le faire. Est-ce qu'ils ont la ténacité ? Il faut passer à un autre paradigme de conformité, de sécurité. Ils ont fait des pas timides au fil des ans et maintenant, ils semblent quand même plus ambitieux et plus décidés. On va les suivre de près avec grand intérêt.

Graeme.

GRAEME BUNTON : Merci. Quelques réactions au sujet de la conformité.

Tout d'abord du côté de la chambre des parties contractantes, nous les avons suffisamment armées, et les indications qu'ils retirent des rapports individuels de la conformité plus les réactions de notre projet Compass par exemple qui nous donnent une idée de l'utilisation malveillante de l'écosystème ou bien du programme à venir de l'ICANN Metrica, cela va leur donner tout ce qu'il faut pour ensuite agir. Et dans ce cas, mon intuition me dit que toute la communauté, les bureaux d'enregistrement, les opérateurs, l'ALAC, le GAC, tout le monde veut voir ces utilisations malveillantes cesser. Je pense qu'ils seront les premiers à l'utiliser.

Maintenant, croyez-moi si je vous dis qu'on pourrait passer un bon moment à parler des différences entre l'atténuation de l'utilisation malveillante, l'accès aux données des titulaires de nom de domaine, l'exactitude quant aux données des titulaires et comment tout cela s'articule. Mais ce qui est important pour moi quand je vois tout cela, et très souvent on fait exprès de ne pas parler de cet accès aux titulaires parce que ça empiète un peu sur la question de la vie privée, etc. et cela complique passablement notre travail, donc on laisse cela de côté. Mais

quand les bureaux d'enregistrement atténuent ces utilisations malveillantes, ils essaient de savoir s'il y a un sondage qui a lieu sur ce site ou sur cette adresse e-mail en en utilisant un nom de domaine. Cela n'exige pas de données sur les titulaires de nom de domaine. C'est très important de ne pas l'oublier.

Beaucoup de registres et de fournisseurs de services au registre ont dit très ouvertement qu'ils font tout ce travail de PII de manière gratuite. Cela ne veut pas dire que ces données n'ont aucune utilité, mais il y a beaucoup de travail qu'on doit faire avant de passer à l'étape d'après.

Et dernier détail. C'est très important, très intéressant pour nous à l'institut, comment est-ce qu'on peut véritablement changer la donne quant à l'utilisation malveillante ? Je divise cela en deux parties principales. Tout d'abord, on a l'amélioration des processus réactifs, est-ce qu'on peut améliorer les processus pour que les opérateurs de registre aient une meilleure qualité plus vite ? C'est l'essentiel. Il y a beaucoup de travail qu'on peut faire pour améliorer ces processus de réaction. Et c'est justement le cœur de ces amendements.

Ensuite, Laureen a expliqué qu'elle était optimiste. Ram a parlé de travail alpha, de travail bêta, en gros c'est le travail embryonnaire de tout ce qui est apprentissage des machines, etc. Moi, je me suis penché là-dessus assez sérieusement. J'ai même fait une présentation au symposium DNS au Vietnam. Si vous êtes vraiment curieux, vous pouvez fouiller un peu. Mais en deux mots, ceux qui ont vraiment publié des travaux sur l'identification des noms malveillants viennent surtout de la communauté des ccTLD, des noms de domaine géographiques, et cela n'a pas été extrêmement réussi. Je crois qu'il n'était pas prêt pour

les feux de la rampe commerciaux, mais cela s'explique surtout par le fait que les registres n'ont souvent pas assez de données pour bâtir un modèle qui sera suffisamment précis et exact. C'est la nature des registres dans l'écosystème actuellement. Je pense que les bureaux d'enregistrement, quant à eux, sont bien mieux positionnés pour se doter de la technologie qui peut identifier les noms de domaine, avant ensuite de passer dans la zone et de faire des dégâts éventuellement. C'est ce qu'on veut. En fait, on veut éviter tout dégât et tout préjudice.

Ensuite, on passe à une autre question très intéressante. J'aimerais bien en discuter avec tous ceux qui s'en soucient. Je m'en soucie de manière presque maladive. Est-ce que c'est bon d'investir dans ce modèle ? Parce que ce modèle sera très cher, ce sera quand même un effort colossal sur le plan des ingénieurs. Ou est-ce qu'on va se pencher sur ce que les bureaux d'enregistrement utilisent déjà ? Ils ont déjà des mesures de détection de fraude très solides qui peuvent être utilisées à peu de frais. Et je pense que c'est plus pratique, plus immédiat. C'est une technologie qui peut être intégrée plus aisément plutôt que de bâtir notre propre modèle très sophistiqué. Je pense qu'il faut y réfléchir sérieusement avant de simplement se jeter à corps perdu. Merci.

GREG SHATAN : Merci. Cela me rappelle ce qu'un bureau d'enregistrement m'avait dit : peu importe ce qu'est le WHOIS, nous avons notre propre base de données que nous utilisons pour connaître notre clientèle. Il y a beaucoup de bureaux qui font cela dans le secteur, je crois que c'est logique. Il y a une grande séparation entre le qui est le quoi. Et le quoi,

c'est l'utilisation malveillante du DNS et le qui, c'est ceux qui pratiquent ces fraudes. En tout cas, nous devons avant toute chose nous centrer sur cette activité malveillante et ensuite voir qui réalise ces activités malveillantes.

Steve, allez-y, vous avez la parole.

STEVE CROCKER : Cette discussion est très intéressante. Quelques commentaires

Lorsque je pense aux données d'enregistrement, je dirais que ce n'est pas toujours ce qui correspond exactement à ce qui est collecté, par exemple à travers le RDRS. Cela conclut les informations pour payer. Cela comprend toute une variété de données qui sont collectées pendant l'enregistrement.

Je dirais que tous ceux qui sont ici dans cette salle ont déjà enregistré un domaine. Lorsque vous voulez obtenir un nom de domaine, vous travaillez avec votre bureau d'enregistrement, vous lui donnez les numéros de votre carte, vous allez sélectionner un nom. Si ce nom est disponible, vous allez l'enregistrer. Ensuite, le bureau d'enregistrement va avoir une autorité sur ce nom. Mais le contrôle physique sur ce nom, c'est la personne qui a créé son compte, qui a payé, etc. On ne parle pas de cela, on ne parle pas de cette relation entre le client et le bureau d'enregistrement. Quand on parlait du WHOIS détaillé ou WHOIS résumé, on ne parlait pas de cela. Et pourtant, il y a une question ici qu'on pourrait se poser.

À nouveau, on a des tendances ici. Un élément important, c'est de voir les données que peut avoir un bureau d'enregistrement et ensuite voir l'environnement dans son ensemble et voir s'il y a quelque chose qui crée des vagues.

Personnellement, je comprends qu'il y a certaines choses qui provoquent des réactions. Mais ici, ce que l'on ne veut pas créer, c'est un énorme chaos. On veut créer un système qui nous permette de le contrôler. Nous devons utiliser le contrôle du secteur financier, certains mécanismes qui existent et qu'ils possèdent dans ce domaine, par exemple la carte de crédit qui a été utilisé, qui a été acceptée pour un paiement. C'est un outil quand on voit qu'une carte de crédit est légale et peut être utilisée pour un paiement par exemple. Il y a toute une série de détails ici qui entrent en jeu.

GREG SHATAN : Merci beaucoup.

Nous donnons maintenant la parole à Reg.

REG LEVY : Merci beaucoup.

Beaucoup de nos clients ne veulent pas que leurs données soient publiées ou distribuées. En plus, je voudrais revenir à une question qui a été posée. Est-ce que l'ICANN a un rôle à jouer dans l'utilisation malveillante de contenu ? Personnellement, je pense qu'il y a des limites, mais que les contenus, c'est quelque chose qui ne dépend pas de l'ICANN. Il y a des choses que les opérateurs de registre, les bureaux

d'enregistrement font. Il y a certaines choses qui ne sont pas sous la responsabilité de l'ICANN, qui sont exactement à l'extérieur de sa responsabilité. C'est inquiétant de voir que l'ICANN change à ce propos.

Est-ce que l'ICANN doit publier son rôle concernant l'utilisation malveillante du DNS ? Oui, je pense que c'est bien. Beaucoup de gens ont entendu parler de l'ICANN et parfois ils ne savent pas ce que c'est. Ce serait bien peut-être que l'on sache ce qu'est l'ICANN. Beaucoup de gens ignorent complètement ce qu'est l'ICANN. Si l'on parle du combat que mène l'ICANN contre l'utilisation malveillante du DNS, beaucoup de gens vont ignorer, ils ne vont pas savoir de quoi il s'agit. Les parties contractantes ont beaucoup de travail concernant ce qu'ils font et expliquer ce qu'ils font, faire de la sensibilisation concernant leur travail, avoir une conversation avec la communauté. Mais je ne sais pas si le public à l'extérieur de la communauté de l'ICANN connaît l'ICANN et sait que l'ICANN représente quand il s'agit de défendre une utilisation honnête de l'Internet.

GREG SHATAN : Jonathan, allez-y.

JONATHAN ZUCK : Je crois qu'on a dit beaucoup de choses intéressantes ici, beaucoup d'approches et des manières intéressantes d'analyser cette question. Je pense qu'il y a des travaux qui ont été faits, des recherches qui ont été faites sur tout cela. Je me souviens pendant la période de la pandémie, cette conversation a eu lieu. Il était difficile de savoir ce qui pouvait être utilisé, ce qui était valide ou pas. En tout cas, la question

liée à la carte de crédit, c'est intéressant. Les enregistrements, la corrélation entre enregistrements de grand volume qui très souvent correspondent à des utilisations malveillantes, les études qui ont été faites concernant l'utilisation malveillante du DNS, tout cela nous amène à quelque chose de concret permettant de lutter contre cela.

Maintenant, j'ai une question. On a parlé de cet amendement qui va entrer en application au mois d'avril et les attentes concernant cet amendement. À partir de là, il y aura une conformité, il y a des attentes concernant et ces fraudes. Est-ce qu'il y a des escrocs qui vont pouvoir faire quelque chose avant le mois d'avril, à votre avis ?

GREG SHATAN : Je ne sais pas.

Nous avons une question à distance. Est-ce que vous pourriez s'il vous plaît la lire ?

MICHELLE DESMYTER : Nous avons une question d'Olivier Crépin-Leblond : « Est-ce qu'on peut avoir une question de message concernant le contenu qui pourrait être diffusée ? »

REG LEVY : Oui, mais c'est le nom de domaine. Et le DNS, c'est le système de noms de domaine. Ce sont deux choses différentes.

GREG SHATAN : Oui, même s'il y a des contenus liés aux noms de domaine. Mais lorsque l'on parle d'utilisation malveillante de contenu, il y a des questions liées à la responsabilité qui pourraient donner lieu à des discussions passionnantes concernant le contenu.

Il y a encore beaucoup de choses intéressantes à discuter, mais je pense que, pour conclure, je dirais que nous avons appris beaucoup de choses concernant l'utilisation malveillante du DNS. Nous avons appris certains détails sur l'amendement qui va commencer à être appliqué à partir du mois d'avril. Nous avons entendu parler du département de conformité, différentes solutions qui peuvent être définies concernant les données d'enregistrement. Il y a différentes préoccupations concernant le temps lié aux atténuations, le fait que ces délais peuvent être très problématiques. Et finalement, ce que Laureen nous a dit, l'objectif final est de défendre l'utilisateur et d'empêcher que ces escrocs volent ou détruisent son entreprise. Quand on parle d'utilisateurs finaux, on parle du public en général avec les tentatives d'hameçonnage et autres. Il y a un monde réel dans lequel les conséquences de ces actes sont graves pour les utilisateurs finaux qui ont tout à perdre. Notre environnement, notre secteur tribunal en souffre aussi. Mais je pense que nous allons pouvoir trouver des moyens de lutter contre tout cela.

Finalement, c'est lié à la nature fondamentale de l'Internet. Le paradoxe de la médiation On ne sait jamais très bien qui est en face de nous. Il y a une série de secrets qui entrent en jeu et on a la possibilité d'être très proches et d'être très loin en même temps. Il n'y a aucune autre méthode de communication qui possède ces paramètres.

L'Internet est très puissant et il peut être utilisé pour des choses très bonnes et très mauvaises.

Est-ce que quelqu'un veut prendre la parole avant que la réunion soit levée ?

RAM MOHAN : Je pense qu'on a dit des choses très intéressantes. Je n'ai rien d'autre à ajouter. Je ne suis pas dans une situation dans laquelle je devrais répéter ce qui a déjà été dit, donc j'en resterai là.

GREG SHATAN : Parfait. Je crois que la discussion a été très enrichissante. On a entendu les commentaires les plus intéressants. Je remercie tous les membres de ce panel pour leur participation. Je crois que ce panel a vraiment couvert tous les thèmes qui étaient à l'ordre du jour. Je vous remercie, je remercie notre public en ligne et dans la salle. Cette réunion est maintenant terminée. Merci.

[FIN DE LA TRANSCRIPTION]