JOHANNESBURG – Session de travail de l'ALAC et des dirigeants régionaux - 5e partie
Mercredi 28 juin 2017 – 13h30 à 15h00 JNB
ICANN59 | Johannesburg, Afrique du Sud

INTERVENANT NON IDENTIFIÉ : Il s'agit de la réunion de l'ALAC et des leaders régionaux, cinquième partie de la séance. Nous sommes le 28 juin, 13 h 30 à 15 heures, Ballroom 4.

ALAN GREENBERG : Très bien, merci. Eh bien, bienvenue à la séance de l'ALAC numéro 5, séance 5. Nous avons trois différents intervenants qui n'ont qu'une demi-heure chacun, donc je veux commencer tout de suite.

Nous allons commencer par Greg Aaron qui va nous parler de l'utilisation malveillante des noms de domaine. Et Greg est une des personnes qui sont un grand spécialiste de cela. Il observe ce qui se passe sur l'Internet. Il essaie de nous protéger. Donc je crois que ça va être quelque chose de tout à fait intéressant. Je ne vais pas l'introduire, le présenter, plus longuement. Je lui donne tout de suite la parole.

GREG AARON : Donc moi, je suis un expert de la sécurité cybernétique. Une de mes spécialités, c'est observer comment les cybercriminels utilisent les noms de domaine. Donc je travaille pour une entité qui s'appelle iThreat. Et je suis également membre de SSAC à l'ICANN et je fais partie du Groupe de travail anti hameçonnage.

Donc nous allons passer à notre premier transparent.

Une manière de définir l'utilisation malveillante : c'est une activité qui requiert ou utilise des noms de domaine pour perpétrer des activités malveillantes. Donc dans cette définition, on peut faire entrer plusieurs points, mais il y a des points qui sont très connus dans la cybercriminalité. Ils utilisent les noms de domaine, mais moi j'utilise ce qui est fondamental. J'étudie ce qui est fondamental. Le spam.

Le spam permet beaucoup aux cybercriminels. Le spam, qu'est-ce que c'est ? C'est envoyer des courriels non sollicités. Dans certaines juridictions, ce n'est pas toujours illégal. Mais je parle d'activités qui sont illégales dans la plupart des cas de figure.

85 % des courriels qui sont envoyés dans le monde, 85 %, sont considérés comme du spam. Et ça vient de robots, de botnets, de machines infectées, d'ordinateurs infectés qui envoient directement ces courriels. Donc ça, c'est une activité criminelle d'utiliser ce type de robot.

Le spam fait de la promotion, c'est de la publicité, pour des choses peu graves ou plus graves. Donc il y a des domaines qui font de la publicité dans le cadre de ce courriel non demandé, de ce spam. Et cela consomme de nombreux noms de domaine chaque année. De 8 à 10 millions de noms de domaine sont utilisés pour ces spams. Donc sur 300 millions de noms de domaine, il y a un pourcentage important qui est utilisé pour les spams.

Pour l'hameçonnage, également, on utilise beaucoup le spam. Lorsque l'on imite un site Web en lequel on a confiance, PayPal, votre banque, et ainsi de suite. Ces malfaiteurs essayent d'inciter les gens à entrer leur carte de crédit, les numéros de leur carte de crédit. Il y a des fraudes qui existent, qui sont nombreuses à ce niveau-là ; les numéros de carte de crédit et les comptes en banque. Et il y a beaucoup de services qui essayent de limiter le nombre de spams que vous recevez. Mais ce courriel indésirable, ce spam, vous connaissez peut-être les princes nigérians qui veulent vous envoyer des centaines de millions de dollars. Ça, c'est aussi une manière illégitime d'utiliser les courriels.

Vous avez les malwares qui vont infecter votre ordinateur, et votre ordinateur va devenir une machine qui envoie sans que vous ne le sachiez des courriels.

Il y a des attaques DDoS où il y a beaucoup de trafic qui est envoyé vers la même destination pour que le service ne fonctionne plus. Donc les activités DDoS sont de plus en plus nombreuses et elles utilisent beaucoup de bande passante. Donc vous avez peut-être entendu parler de caméras de sécurités qui sont utilisées pour ce type d'activité. Parce que là aussi, il y a des logiciels malveillants qui vont infecter ces machines.

Donc ça, c'est très courant. C'est assez bien compris. Et ce sont des activités criminelles à la base. Il y a un consensus là-dessus.

Donc transparent suivant.

Ça, c'est un exemple du suivi qui est effectué dans la communauté de sécurité. Moi, je le fais avec le groupe anti hameçonnage, et ça montre le nombre d'attaques d'hameçonnage, le nombre d'attaques d'une année sur l'autre, ou d'utilisation malveillante des noms de domaine.

Donc là, vous voyez le nombre de sites qui sont utilisés, des sites d'hameçonnage. C'est une croissance qui multipliée par cinq depuis 2008. Là aussi, il y a des noms de domaines qui sont inscrits pour ce faire en 2016. C'était la première fois que nous avions vu des noms de domaine inscrits en grand nombre pour faire de l'hameçonnage, parce qu'ils essayent d'avoir accès à certains sites Web et ils essayent, ces malfaiteurs, de rentrer

dans le site Web de quelqu'un d'autre et utiliser ce site Web pour faire de l'hameçonnage. Mais là, maintenant, c'est assez nouveau ; les malfaiteurs qui font de l'hameçonnage achètent des noms de domaine. Par exemple, certains bureaux d'enregistrement en vendent beaucoup plus. Et il y a certains TLD où il y a de plus en plus d'activités malfaisantes et malveillantes. Donc pour protéger contre cela, ça devient un problème. Il y a beaucoup plus de vulnérabilité dans certaines régions que dans d'autres.

Alors, la réalité de cette cybercriminalité. Comment devons-nous protéger nos clients et quel est le nouvel écosystème ? Comment est-il organisé ?

Donc à la base, ce type d'activité est très professionnel. Beaucoup plus qu'avant. Ce sont des spécialistes. Il y a quelques amateurs dans le lot, mais de plus en plus de professionnels. Ils gagnent des millions de dollars chaque année grâce à cela. Ils volent des millions de dollars des entreprises et des citoyens.

Donc les comptes en banque, et ce n'est pas des comptes en banque de particuliers où il y a quelques centaines de dollars ; des dizaines de milliers de dollars sont parfois subtilisées sur des comptes en banque. Donc certains bureaux d'enregistrement et registres et certains fournisseurs de services concentrent cela parce qu'ils ne sont pas très prudents. Ils sont inattentifs ; il y a

quelqu'un dans leur personnel qui ne gère pas cela. Il y a un problème de prévention. Il faut connaître vos clients et il faut s'assurer que les prestataires de services ne laissent pas ces criminels utiliser leurs services d'enregistrement. Il faut que les entreprises soient plus proactives pour contrôler la situation.

Donc l'inattention est un problème. Les prix les plus bas c'est un autre problème. Les prix cassés. Avec les nouveaux TLD, il y a des noms de domaines qui sont devenus très bon marché. Il y a beaucoup de concurrence dans le secteur, dans notre secteur industriel et des millions de noms de domaine ont été vendus dans les nouveaux TLD spécialement pour le spam. Ça, c'est un problème qui attire les criminels. Ils ne veulent pas payer beaucoup ; ils sont un petit peu avares ces criminels.

Il y a parfois, chez certains prestataires de services, des personnes qui sont complices ou qui sont même des criminels. Il y a eu des bureaux d'enregistrement qui essayait d'avoir pignon sur rue pour justement avoir un grand nombre de domaines, [S Domains] je crois, ça s'appelait comme cela. La personne a été condamnée en Estonie. Et ABSystems utilisait son bureau d'enregistrement pour faire du spam et vendre des produits pharmaceutiques de manière illégale. La personne a été arrêtée par les Américains, et c'était quelqu'un qui était prêt à tuer pour continuer à faire son travail.

Et ils connaissent très bien les noms de domaine. Le système des noms de domaine. Ils ne vont pas jouer le jeu ; véritablement, ce sont des gangsters.

Alors la protection est faite principalement pas par les forces de l'ordre. Les forces de l'ordre sont extrêmement importantes, j'en conviens, mais néanmoins non pas les ressources, non pas le temps de bien poursuivre les problèmes. Ils ne peuvent pas s'occuper des petits joueurs. Ils doivent s'occuper des affaires où il y a beaucoup d'argent en jeu et beaucoup de criminels. Ils vont s'intéresser à ces activités. Ils travaillent très dur, mais ils n'ont pas la possibilité d'avancer très vite. On ne peut pas leur demander de tous nous protéger. C'est absolument impossible.

Donc les relations sont gouvernées par des contrats. Si vous voulez utiliser un service comme Google ou Skype, vous avez des termes de service pour votre téléphone portable, pour votre ISP. Ce sont des contrats qui sont signés et qui disent quels sont les termes de service du contrat. Qui nous donnent le droit donc, et qui leur donnent le droit également si vous y allez les termes de services, de fermer le contrat, de clore le contrat. Donc il y a des personnes dans le secteur de la sécurité qui vont, par exemple, appelé un bureau d'enregistrement ou un registre en disant qu'il y a quelque chose qui se passe, il faut que vous agissiez ; il y a un site d'hameçonnage, il faut que vous retiriez cette page Internet.

Donc il y a une coopération qui est faite et qui existe lorsqu'il y a des contrats, lorsqu'il y a des termes de service dans cet environnement concurrentiel. Donc dans mon secteur, toutes les personnes qui opèrent des ressources Internet ont une responsabilité que de faire respecter ces contrats et de prendre en compte les personnes qui ont été des victimes. Parce que l'Internet est un réseau de réseaux et il n'y a pas véritablement d'entités qui gouvernent l'Internet, qui contrôle tout sur l'Internet. Donc on fait de notre mieux pour s'attaquer. C'est excellent que l'Internet soit ouvert, mais la cybercriminalité est un problème et véritablement un inconvénient de ce système décentralisé.

Donc quel est le rôle de l'ICANN dans tout cela ? Eh bien, c'est ce que je pense personnellement.

Nos statuts nous disent que la mission de l'ICANN, comme vous le savez, les attributions de l'ICANN c'est de s'assurer de l'opération stable et sûre du système d'identifiant unique de l'Internet, avec des politiques pour une résolution coordonnée uniforme étant nécessaire pour faciliter l'ouverture de l'Internet et ainsi de suite.

Donc vous connaissez tout cela. Donc l'ICANN accrédite les registres et les bureaux d'enregistrement et donne le droit de vendre des noms de domaine, accorde des permissions. Mais il y

a des politiques qui existent dans les contrats. Nous avons, comme vous le savez, beaucoup de procédures à ce niveau. Procédures d'accès par exemple aux zones, aux fichiers de zone. Et l'ICANN est en mesure d'avoir beaucoup d'informations sur l'infrastructure et sur la manière dont est organisée l'infrastructure. L'ICANN indique bien dans son contrat qu'on ne peut pas utiliser de manière malveillante les noms de domaine. Il est contrat de l'ICANN sont contraignants. Ça, c'est très important. Ce sont des contrats contraignants.

Ce que je suggère, c'est qu'il faut se concentrer sur les plus grands problèmes, les problèmes les plus importants. La plupart de ces enregistrements malveillants sont faits dans certains endroits. Il faut comprendre pourquoi ça se passe dans ces endroits. Il faut essayer vraiment d'améliorer la situation.

Donc pour la fin de ma présentation, je suis prêt à répondre à vos questions.

ALAN GREENBERG : Eh bien, je l'espère. Andrei.

ANDREI KOLESNIKOV : Oui merci. Oui, Greg. Je crois que c'est très important de dire, les utilisations malveillantes des noms de domaine font partie d'une cybercriminalité encore plus large, une criminalité qui

représente des milliards de dollars. Et ce n'est pas seulement quelques criminels qui font cela. C'est tout un système, je pense, qui est une économie noire sous-jacente, comme je l'ai dit, de milliards de dollars.

Et je crois véritablement qu'on aura besoin d'outils en ligne qui aident les bureaux d'enregistrement à obtenir les données sur l'utilisation des noms de domaine. Et ça va plus loin que les gTLD. C'est très important pour les ccTLDs également.

Et vous savez que .RU je l'ai géré il y a de cela de nombreuses années. Il y avait des outils en ligne où on pouvait faire des contrôles sur l'Internet, effectuer des rapports, générer les rapports. Mais pour ce faire, on a besoin de financement évidemment.

Les grands registres et les registres très importants des gTLD peuvent se le permettre. Peuvent se permettre de créer ce type d'outils. Nous l'avons fait sur une base non commerciale. Nous avons financé ce revenu en tant que registre national.

Mais est-ce qu'il y a – ma question sera – est-ce qu'il y a des services pour les bureaux d'enregistrement et les registres, pour avoir des outils pour lutter contre les botnets et ainsi de suite ? Combien de systèmes existe-t-il ? Parce que ça fait sept ans déjà écoulés depuis que j'ai travaillé à cela. Donc je ne sais plus exactement quelle est la situation.

ALAN GREENBERG : Il ne reste que 15 minutes. Deux minutes limite pour chaque intervention.

GREG AARON : Eh bien, les bureaux d'enregistrement et les registres utilisent des données différentes. Et certains d'entre eux sont très au courant de ce qui se passe, d'autres moins. Ce que je dirais, c'est qu'ils ont besoin de mettre ça dans leur budget. Ces informations sont extrêmement importantes pour atténuer les risques et pour en fin de compte améliorer leurs performances. Ils peuvent obtenir ces outils de différentes manières.

ALAN GREENBERG : Olivier.

OLIVIER CRÉPIN-LEBLOND : Donc, ça, c'est un des thèmes. Moi je suis EURALO, et ça, ça m'angoisse beaucoup lorsque je parle de cela depuis tant d'années à l'ICANN. C'est un thème est un sujet qui heurte et qui fait du mal aux utilisateurs finaux et l'ICANN ne fait pas assez à ce niveau.

L'ALAC a toujours noté qu'il fallait lutter contre les chaînes qui étaient sensibles, pour qu'il y ait plus de sécurité, plus de

vérification des bureaux d'enregistrement. On nous a repoussés très souvent. Les entités commerciales veulent vendre ces chaînes sensibles sans aucun problème, sans plus de sécurité.

Mais j'ai fait beaucoup de suivi du Groupe de travail anti hameçonnage, et je vous félicite pour votre travail. Je crois que ce matin je vous ai envoyé un article sur votre rapport. La situation empire fortement.

En 2015, on parlait aux entités contractuelles. On parlait des nouveaux gTLD. On parlait d'anti hameçonnage et ainsi de suite. Et au jour d'aujourd'hui, on voit toutes ces attaques informatiques qui existent.

J'ai envoyé aussi une note à d'autres groupes de travail pour demander que l'on fasse, dans les contrats avec les bureaux d'enregistrement, plus pour qu'on puisse rapidement limiter ces sites Web, les stopper, les retirer. Donc je crois qu'on s'est en effet qu'il y a certains pays qui sont plus néfastes que d'autres. Qu'est-ce qu'on peut faire pour cela ?

GREG AARON : Eh bien, l'atténuation, c'est quelque chose que les bureaux d'enregistrement des registres doivent prendre en compte dans leur budget. Mais ce n'est pas toujours le cas. Et la concurrence

dans cet espace est intense en ce moment. Tout particulièrement, si les domaines sont vendus très peu cher.

Donc on voit que ça se déplace, ces utilisations malveillantes, d'un endroit à un autre. Ça dépend beaucoup des prix par exemple.

Et lorsque vous avez une chaîne qui est en rapport avec une activité, par exemple il n'y a pas le nom d'une entreprise, les hameçonneurs vont utiliser ce qu'ils veulent.

Ce qui m'inquiète le plus, c'est lorsqu'il y a beaucoup de noms de domaine qui pose problème. C'est un problème de conformité. Nous avons certains outils. Est-ce qu'on a besoin de plus d'outils ? Est-ce que nous avons besoin, dans nos contrats de service SLA, de pouvoir retirer ces noms de domaine ?

Les bureaux d'enregistrement responsable ont parfois du mal à tout gérer. Donc je crois que la conformité est l'un des meilleurs outils que nous avons à notre disposition. Je ne sais pas si on l'utilise à bon escient.

OLIVIER CRÉPIN-LEBLOND : Trois mots : c'est vraiment très dommage.

ALAN GREENBERG : Une minute et demie maintenant pour les questions ; nous n'avons que très peu de temps. Donc Harold.

HAROLD ARCOS : Oui merci. Je vais parler en espagnol. Vous m'entendez ? Merci. Greg, merci pour votre présentation.

Je voulais, parce que je sais que ce qui est arrivé hier au niveau mondial est un bon moment pour poser une question que des utilisateurs finaux m'ont posée lors de réunions précédentes ; hier, une attaque massive a eu lieu. La deuxième après le WannaCry dans plusieurs pays qui ont dit qu'ils ont été attaqués, l'Inde, la Russie, certaines entreprises du Royaume-Uni.

Les usagers me demandent que fait l'ICANN à ce propos ? Est-ce que c'est sa responsabilité d'ajouter des politiques dans les contrats, qui tiennent compte de cela ?

Et cette présentation que l'on vient de nous faire montre qu'il y a des politiques en ce sens. Mais il n'y a pas une connaissance précise de ce qui arriverait si on ne respecte pas ces exigences. Et ce qui s'est passé hier a un impact sur ICANN. On peut se demander qu'est-ce qu'on peut faire, ou bien, en tout cas, mettre en place ce type de contrat. Merci.

GREG AARON : Vous parlez de l'attaque de demande de rançon qui a eu lieu hier. Je sais que c'est un type d'attaque typique, et l'atténuation a lieu de deux manières. La lutte contre cela a lieu de deux manières. Le registre ou le bureau d'enregistrement fait un appel. On peut aussi essayer de trouver cette information si on contrôle des listes bloquées, des listes de blocage ou des listes noires qui sont disponibles. Certaines sont gratuites, d'autres non. Mais il y a des sites qui fournissent ces données. D'autres bureaux d'enregistrement les utilisent. Donc on peut fermer ces domaines s'ils font ce type de choses.

Certaines de ces activités sont difficiles à détecter, d'autres se répandent dans le monde entier. Les criminels qui font ce type d'activité vont avoir les forces de l'ordre qui vont les poursuivre, parce que ça s'est répandu et c'est international. Et cela peut prendre un moment pour que les forces de l'ordre les trouvent, mais les forces de l'ordre vont les poursuivre. Ça, c'est sûr.

HAROLD ARCOS : Excusez-moi, Alan. Est-ce que je peux continuer ?

Au-delà des agences de sécurité et des forces de l'ordre, où est-ce qu'ICANN cherche des informations quand ce type de chose a lieu ? Les agences de sécurité, les forces de l'ordre ont un rôle à jouer au sein des pays, mais ICANN, que fait ICANN dans ces cas-là ? Comment fait ICANN pour faire un suivi ?

GREG AARON : Les équipes de sécurités d'ICANN obtiennent des informations par de tierces parties parce que des fois on a besoin de trouver les bonnes personnes à qui parler. On a besoin de contact dans un registre. L'équipe ICANN va faciliter son contact.

ICANN commence aussi à recevoir des données consolidées concernant tout cela. Et, en tant que contractant, je les aide.

ALAN GREENBERG : Dave Piscitello.

DAVE PISCITELLO : Je suis de l'équipe de sécurité d'ICANN, Greg.

Je me demandais si vous pouviez faire un commentaire sur l'amplification d'un nom de domaine en de nombreuses URL, parce que le nom de domaine c'est un seul vecteur est très souvent ils représentent seulement une fraction du grand nombre d'attaques qui ont lieu en réalité.

GREG AARON : Dave parle des cas où il y a plusieurs acteurs qui peuvent, par exemple, mettre différentes choses sur un nom de domaine dans lequel ils rentrent ; ils peuvent mettre cela dans un fichier. Ils peuvent aussi rentrer dans le DNS de votre nom de domaine

individuel, envoyez cela à différents sous-domaines. Donc un nom de domaine peut être utilisé pour perpétrer différents types de délits ou d'attaques. Et c'est important de le savoir.

Nous devons aussi savoir que certains noms de domaine soutiennent plusieurs services, et que leur compagnie se consacre à vendre des sous-noms de domaine. Donc on ne veut pas fermer ces noms de domaine, parce qu'à ce moment-là, on annule tous les services qui fonctionnent. Donc c'est un des défis pour ce type de problèmes. On ne veut pas, des fois, causer plus de mal que de bien.

ALAN GREENBERG : Très bien. Nous sommes un peu en retard. Nous avons deux autres personnes qui voudraient prendre la parole. Kaili et Alberto, est-ce que vous pouvez être brefs parce que nous avons deux autres très intéressants.

KAILI KAN : Merci Alan. Je serai bref. Kaili Kan. J'appartiens au CCTRT pour le choix du consommateur, l'équipe de révisions pour les nouveaux gTLD. Je voudrais savoir cette utilisation malveillante du DNS, comment est-ce qu'elle fonctionne avec le programme des nouveaux gTLD. Est-ce que cela peut avoir un impact ou un effet sur les utilisations malveillantes du DNS ? Et concernant les

discussions au sein de l'ICANN actuellement, pour les procédures ultérieures pour les nouveaux gTLD, et s'il y a quelque chose que l'on peut faire pour prévenir davantage d'utilisations malveillantes du DNS et que cela soit inclus dans la prise de décision politique.

GREG AARON : Une question que l'on peut se poser, c'est à ce que les nouveaux TLD, nouveaux gTLD, créent davantage de cyber délits. On peut se demander aussi est-ce que les nouveautés TLD permettent à un grand nombre d'activités et de s'installer, activités malveillantes.

KAILI KAN : C'est justement la question que je vous pose.

GREG AARON : On voit beaucoup de preuves selon lesquelles les nouveaux gTLD ont attiré beaucoup de ce type d'activité. On le voit au niveau du spam. On le voit au niveau de l'hameçonnage. On est en train d'essayer de mesurer tout cela.

Ce que cela signifie, c'est qu'il faut travailler avec les opérateurs, avec ses registres, avec les bureaux d'enregistrement. Il faut

comprendre pourquoi ils sont allés là. Les prix bas sont souvent une raison.

L'autre question est, est-ce que les nouveaux gTLD créaient davantage de cyber délits. Je ne pense pas. Il y a beaucoup de noms de domaine dans les gTLD, dans les ccTLD. Les criminels peuvent avoir autant de noms de domaines qui le veulent, peu importe à quel secteur cela appartient.

Il faut voir ces six nouveaux programmes gTLD à créer de nouveaux opérateurs, et à ce moment-là est-ce qu'on peut les joindre ? Est-ce qu'ils font du bon travail ? Voilà ce qu'on peut se demander, ce qu'on peut se poser comme question.

ALAN GREENBERG : Très bien. Alberto, vous avez la parole.

ALBERTO SOTO : Je vais parler en espagnol.

Je comprends et je pense que vous devriez travailler avec le GAC aussi. D'accord ? Parce que j'aimerais savoir que répond le GAC face à vos avertissements concernant l'utilisation malveillante des noms de domaine. Parce qu'ICANN ne peut pas s'occuper de cela, mais chaque pays peut prendre des mesures, des

dispositions efficaces dans ce sens. Ce qui n'a pas été le cas jusqu'à maintenant.

GREG AARON : Merci. Dans le GAC, il y a quelque chose qui s'appelle le Groupe de travail sur la sécurité publique qui est formé de représentants des forces de l'ordre, de régulateurs entre autres, qui donnent des conseils au GAC concernant les avis du GAC à ICANN concernant le cyber délit. Et ils ont demandé à ICANN de mettre en œuvre certaines politiques comme, par exemple, la politique concernant l'exactitude du WHOIS, les politiques de contrôle en cas d'utilisation malveillante. Donc ils travaillent. Ils essayent de mener le GAC à donner un avis à l'ICANN, et ensuite ils donnent des conseils au gouvernement de manière individuelle. Et cela est très important.

ALBERTO SOTO : Ma question, ce n'est pas ça. Je comprends que vous parliez de ce qui se fait au sein de l'ICANN. Mais ma question c'est dans votre groupe, au niveau du GAC, qu'est-ce que vous recommandez pour que les gouvernements respectifs réagissent ?

GREG AARON : Une des choses que les pays pourraient faire, qui pourrait être utile, ce serait que les pays mettent en place des moyens pour les forces de l'ordre leur permettant de coopérer, d'échanger des informations avec les services de l'ordre d'autres pays, parce que bien sûr le cyber délit dépasse les frontières nationales. Les agents des services de l'ordre doivent parler à leurs homologues dans d'autres pays. Donc ils ont besoin de loi leur permettant de le faire. S'ils ne peuvent pas échanger les informations et parler les uns avec les autres, ils ont les poignées – ils ne peuvent rien faire. Ils sont paralysés.

ALAN GREENBERG : Bien. Merci beaucoup. Je vous remercie, Greg. Je pense que cette réunion a été très intéressante et pleine d'informations. Je vous remercie. Merci pour toutes les questions qui ont été posées par la salle. Je crois qu'on est un peu en retard.

GREG AARON : Si vous avez des questions à poser, cherchez-moi dans les couloirs et je serais ravi d'y répondre.

ALAN GREENBERG : Parfait. Nous allons entendre Jonathan Zook, membre de l'équipe des CCT. L'équipe de révision des CCTRT, s'il vous plaît, venez vous asseoir ici.

Je crois que nous n'avons pas besoin de présenter le thème. On en parle souvent. Et nous avons Kaili dans la salle qui nous a fait des rapports réguliers.

Jonathan, est-ce que vous voulez vous présenter ? Présenter les autres personnes qui sont dans la salle ? Nous dire ce se passe ? Je sais que vous avez eu un week-end très intéressant.

JONATHAN ZOOK : Merci Alan. Merci à tous d'être ici et de parler du choix du consommateur, de la confiance et de la concurrence. Je suis Jonathan Zook. Je suis le président du CCT.

Et ici, vous avez le président de la sous-équipe qui travaille sur la confiance et les protections. Vous avez ici le monsieur de Google, qui est le président de l'équipe et qui travaille sur la concurrence et le choix. Et puis, vous avez aussi le président de la sous-équipe qui travaille sur l'évaluation, l'application et la révision.

Donc nous avons eu une réunion présentielle ce week-end. Et nous avons parlé d'une série de définitions. Mais nous nous sommes principalement focalisés sur deux aspects. D'abord, les commentaires publics que nous avons reçus, y compris d'ALAC. Et nous avons essayé d'analyser les problèmes de premier

niveau au cours de la plénière et ensuite dans notre sous-équipe pour, donc, analyser les commentaires et recommandations.

Nous avons aussi eu une présentation en termes d'abus du DNS, un rapport de notre commission. Et donc, nous serons ravis en parler aussi.

Et nous avons ici le responsable de l'utilisation malveillante du DNS. Nous attendons un rapport vers la mi-juillet.

Et nous avons aussi parlé d'une enquête qui a été faite par INTA sur les coûts des titulaires de marques dans le programme de nouveaux gTLD et comment intégrer ces résultats dans notre travail.

Bien. Il y a un autre problème concernant le commentaire d'ALAC. C'est le problème du parking. On a parlé de cela aussi pendant tout le week-end. Donc pendant la réunion de ce week-end.

Donc je ne sais pas comment est-ce que vous voulez que l'on continue. Lorraine, est-ce que vous voulez nous parler un petit peu de tout cela ? Allez-y.

ALAN GREENBERG : Nous avons une demi-heure. En réalité, nous avons 20 minutes. Donc nous ne pouvons pas trop nous retarder. Nous avons un autre orateur sur les noms de domaine.

JONATHAN ZOOK : Bien. Parfait. Je vais respecter tout cela.

Nous avons encore en train d'analyser les commentaires publics que nous avons reçus. Nous apprécions le commentaire d'ALAC qui, pour nous, a été un soutien concernant la confiance du consommateur et les recommandations en ce sens. Donc nous avons apprécié cela et nous partageons vos préoccupations concernant le manque d'information concernant le niveau de confiance que le consommateur a envers le DNS et les nouveaux gTLD en particulier. Et nous espérons que nous allons obtenir davantage d'informations suite à ces recommandations ou à cette recommandation.

Nous travaillons dans le but de rédiger notre rapport final de façon à ce que ce processus soit terminé. Je pense que ce sera vers la réunion d'Abu Dhabi.

Mais il y a deux choses qui vont être importantes. D'abord, il va y avoir un commentaire qui va refléter les résultats des études. Et moi, personnellement, je me focalise surtout sur l'utilisation malveillante du DNS. Et je voudrais mettre l'accent sur le fait que

la version finale de cette étude sera présentée à la fin du mois de juillet et nous incorporerons les résultats de cette étude dans notre rapport. Il y aura des rapports qui seront présentés aux commentaires publics, des parties de ce rapport qui sont présentées aux commentaires publics.

ALAN GREENBERG : Je pense que ce sera très intéressant. Et Jonathan, vous avez la parole.

JONATHAN ZOOK : Je voudrais parler un petit peu des résultats de cette enquête. J'ai vu la dernière partie de la présentation que vous venez de voir. Je crois qu'on va voir beaucoup d'études avec des résultats similaires concernant les mouvements de l'utilisation malveillante des gTLD plutôt qu'une croissance de ses activités.

Il pourrait peut-être même y avoir des activités et des résultats intéressants concernant la recherche sur les nouveaux gTLD.

DREW BAGLEY : Je crois que c'est le bon moment de parler de tout cela.

HEIDI ULLRICH : Excusez-moi de vous interrompre. Je voudrais vous rappeler que nous avons des services d'interprétation en trois langues.

Donnez votre nom quand vous prenez la parole de façon à ce que les participants à distance et les interprètes puissent savoir qui prend la parole. Merci.

DREW BAGLEY : Drew Bagley, de l'équipe de révision des CCT. Donc maintenant, nous avons un rapport préliminaire. Nous recevrons davantage d'informations dans un mois. Mais jusqu'à maintenant, ce que nous pouvons voir, ce qui nous paraît intéressant vu le mandat de notre équipe, c'est que le taux d'action malveillante a été le même après l'introduction des nouveaux gTLD. Donc les actions malveillantes augmentent au même rythme que les enregistrements.

Mais nous avons analysé cela pour savoir s'il y a une substitution qui a lieu. Si les gens passent des gTLD historiques aux nouveaux gTLD pour un certain type d'action malveillante. Et malgré les nouvelles protections qui existent dans le cadre des nouveaux gTLD, d'après les résultats préliminaires que nous avons obtenus, il ne semble pas qu'il y ait de prévention de l'utilisation malveillante des nouveaux gTLD. Mais nous aurons beaucoup d'autres données. Nous pouvons tirer davantage d'informations de l'analyse de ces données je pense que ce sera très bientôt.

Autre point important c'est que le type d'utilisation malveillante, dans le cadre des nouveaux gTLD, d'après le

rapport initial, concerne surtout le spam. Le spam est plus prévalant dans les nouveaux gTLD que dans les gTLD historiques. Donc il semble qu'il y ait une migration qui est donnée lieu à cette croissance.

Un autre point important c'est que les nouveaux gTLD tendent à avoir davantage de noms de domaine malveillants enregistrés, plutôt que des sites Internet compromis qu'on utilise pour ce type d'utilisation malveillante.

Nous espérons que nous pourrons vous donner davantage de détails bientôt, le mois prochain, sur toutes ces questions.

ALAN GREENBERG : Merci. Donc on va laisser les intervenants s'exprimer, ensuite on va leur poser des questions. Et Holly sera la première pour les questions.

JONATHAN ZOOK : Donc, en résumé, je sais que vous avez une question qui brûle les lèvres. Mais on a parlé du parking et du problème que cela posait et des contributions qu'on pouvait faire avec vos commentaires, obtenir de vos commentaires. C'est vu comme une utilisation malveillante que de parquer un domaine de cette manière.

Cela a trait également à la concurrence des nouveaux gTLD. Donc Drew va peut-être rebondir là-dessus au niveau de l'abus du DNS. Donc Jordyn en premier ?

JORDYN BUCHANAN : Oui bien sûr. Brièvement, je vais parler des deux points ; on a beaucoup parlé avec Drew d'ailleurs.

Jordyn Buchanan de Google.

Dans les commentaires de l'ALAC, vous avez noté que le taux de parking dans les nouveaux gTLD est très élevé ; au niveau de 60 % pour les nouveaux gTLD. Donc ça dépend de la méthodologie qui est utilisée, mais c'est significatif, ce taux de parking.

Nous avons passé ces derniers mois à essayer de faire deux choses, depuis la publication du rapport. Voir comment cela se compare par rapport aux autres gTLD. Et nous avons été en mesure d'avoir des données et d'utiliser la même méthodologie pour les anciens et pour les nouveaux gTLD. Nous avons vu que le taux de parking pour les gTLD historiques étaient, je crois, de 40 à 48 %, ce qui est très élevé aussi, mais pas aussi élevé que les 60 % que nous voyons avec les nouveaux gTLD. Donc on s'est dit qu'est-ce que ça veut dire cette différence.

Eh bien, deux points de vue. Cela a trait à la concurrence et à l'utilisation malveillante du DNS. Donc problème de confiance pour le consommateur. Donc il y a eu une hypothèse de notre équipe de travail. Si [inaudible] domaines, il n'y a pas de renouvellement des domaines aussi fréquent. Donc c'est pour cela qu'il y a beaucoup de domaines parqués. Et on ne sait on aura une base stable à l'avenir et si nos résultats donc sont bons.

Pour les taux de renouvellement, on doit trouver une corrélation éventuelle entre le taux de renouvellement et les taux de parking. Dans notre premier test, on n'a pas été en mesure de trouver une corrélation entre les deux, entre les taux de parking et les taux de renouvellement. Donc on essaie de comprendre les éventuels rapports qui existent entre ces différents points. On n'a pas d'autres hypothèses à tester pour le moment. Mais je crois qu'on doit faire plus d'études à ce sujet.

En ce qui concerne la confiance du consommateur, ce n'est pas dans notre rapport préliminaire, mais ça a été analysé. Il y a une certaine corrélation pas très marquée entre les sites de parking, donc les domaines avec des erreurs qui n'ont pas de serveur de domaine, et ainsi de suite. Donc les TLD de ces sites tendent à avoir plus d'utilisation malveillante associée avec eux. On ne comprend pas encore pourquoi ; on ne comprend pas tous les facteurs. On essaye de les découvrir. Est-ce de prix des TLD, le

prix très bas de certains TLD ? Donc on doit savoir plus. On doit continuer à avancer dans notre recherche.

ALAN GREENBERG : Oui merci. On aura 90 secondes uniquement pour les questions. Holly Raiche est la première à poser une question.

HOLLY RAICHE : Oui. Donc quel type d'abus est le plus commun avec les nouveaux gTLD, et quel type d'utilisation malveillante ? Et pourquoi est-ce qu'il y a plus d'utilisations malveillantes donc qu'est-ce qui se passe avec les nouveaux noms de domaine ?

DREW BAGLEY : Dans le rapport préliminaire, nous notons pour le spam, le spam est beaucoup plus prévalant avec les nouveaux gTLD par rapport aux gTLD historiques.

Mais la manière dont l'utilisation malveillante est effectuée – ce sera mon second point –, les données montrent que les nouveaux gTLD, les zones des nouveaux gTLD ont plus de noms de domaines qui ont été enregistrés pour des motifs fallacieux, pour faire du phishing, du hameçonnage, du botnet. Tandis que pour les TLD historiques, c'est à partir d'un site Web légitime qui

était compromis et à partir duquel on faisait de l'utilisation malveillante et du piratage.

Donc ça, ce sont nos premières données, nos données préliminaires. On ne sait pas encore pourquoi. Donc on a une théorie. Ça peut être le prix ; il y a beaucoup de prix très bas pour les nouveaux gTLD. Et les criminels aiment faire des économies.

HOLLY RAICHE : Pourquoi vous nous dîtes ils ont inscrit ? Pour cette raison précisément ?

DREW BAGLEY : C'est sur la base d'un modèle que les chercheurs ont employé pour le rapport qui a été fait sur l'utilisation malveillante du DNS. Donc après l'enregistrement d'un domaine, combien de temps ça prend pour qu'il commence à poser un problème ? Donc ils expliquent cela, les chercheurs, dans le rapport préliminaire. C'est assez complexe. Et le modèle était basé sur une étude d'il y a quelques années et qui a montré qu'il y a des points communs entre les noms de domaine inscrits par des personnes avec de mauvaises intentions et les abus du DNS.

ALAN GREENBERG : Oui. Merci. Question pour Jordyn. Si j'enregistre Hilton.hotels et que je redirige cela vers Hilton.com, est-ce que c'est du parking ? Et quel est le pourcentage de domaines parqués qui sont parqués de cette manière ?

JORDYN BUCHANAN : Merci. Nous avons une définition très large de parking. Tout ce qui n'a pas de contenu, qui est directement hébergé sur ce domaine, pas de DNS, page parquée et ainsi de suite. Donc oui, votre exemple faisait partie du parking. C'est un petit pourcentage des activités de parking. C'est de la redirection. 8 % ; entre 4 et 8 %. Ce n'est pas une majorité des problèmes.

ALAN GREENBERG : Merci. Satish, je vous donne la parole. Question ?

SATISH BABU : Merci Alan. J'aimerais savoir s'il y a, pour les IDN, les noms de domaine internationalisé, est-ce qu'ils sont plus particulièrement susceptibles à l'utilisation malveillante ?

DREW BAGLEY : Oui. Dans le cadre du rapport préliminaire, on n'avait pas de données là-dessus. Et c'est vraiment une question qui nous intéresse beaucoup, évidemment, parce que ces attaques, en

effet, ont des caractéristiques précises. Et nous devons avoir plus de données sur les IDN. Je ne sais pas si les chercheurs ont fait beaucoup là-dessus, mais je peux revenir vers vous sur ce sujet.

ALAN GREENBERG : Merci. Olivier ?

OLIVIER CRÉPIN-LEBLOND : Excusez-moi d'être provocateur, mais nous avons une visite avant vous de David Aaron, du Groupe de travail anti hameçonnage. Ils ont beaucoup de données sur ça. Et je vois que mon collègue encore plus de données. Mais que fait l'ICANN ? On a toutes ces données. Est-ce qu'on va utiliser ces données pour faire quelque chose ? Parce que, pour le moment, c'est une thèse philosophique sur la vie sexuelle d'une balle de ping-pong. Ce que je veux dire par là, beaucoup de données, mais pourquoi ?

ALAN GREENBERG : Oui, je vais laisser Drew répondre à cette question très intéressante.

DREW BAGLEY : Oui. Je suis prêt à répondre. Et je dirais que nous sommes tous très inquiets de cela. Ce que nous faisons avec les recommandations en général c'est d'avoir une approche basée sur des données à l'ICANN.

Donc en ce qui concerne l'utilisation malveillante du DNS, c'est la première fois qu'on a une analyse complète, avec beaucoup de données, pour baser nos politiques et nos décisions. Il y a beaucoup de groupes de travail qui font un excellent travail, mais il y a eu une analyse historique de toutes les zones.

Et notre intention, c'était de mesurer les protections mises en place et à mettre en place et voir si la confiance du consommateur va être impactée pour les nouveaux gTLD. Est-ce qu'on est en ligne avec la réalité des noms de domaine, perçue par les consommateurs.

Et dans le rapport final, on va faire des recommandations de politique sur la base des données. Donc ce n'était pas une étude philosophique sur la vie sexuelle d'une balle de ping-pong, non. C'étaient beaucoup plus des stratégies possibles pour justement régler ce problème.

LAUREEN KAPIN : Oui. Pour rebondir là-dessus, le scénario idéal serait que lorsqu'on a des données spécifiques, cela montre des

comportements, définit des comportements d'hameçonnage éventuellement, d'autres problèmes d'utilisation malveillante. Et que cela va avoir un impact sur le développement de politiques. Le GAC va se pencher là-dessus et va réfléchir au rapport entre les prix par exemple et les abus du DNS. Peut-être qu'on va plus renforcer nos contrats pour des contrats plus solides. Il y a d'autres réponses. Ça, c'est très concret. Par des manières concrètes, on va utiliser ces données pour que ça ne soit pas simplement un exercice de collecte de données qui est positif, mais néanmoins véritablement on va voir si ça tient la route, si on peut sanctionner les problèmes.

JONATHAN ZUCK : Oui. J'aimerais rebondir là-dessus avec cette balle de ping-pong. Il y a différents problèmes. Les problèmes de prix par exemple. Donc c'est la troisième voie qui est la voie où le train prend son électricité qui est très dangereuse. Donc ça, c'est un thème très sensible. L'ICANN n'est pas là pour réguler les prix, n'est pas une entité de régulation des prix.

Mais il y a une [propensité] également pour le spam qui n'est pas uniforme, n'est pas toujours considérée comme illégale. Ça dépend des juridictions au niveau mondial. Donc, en effet, le spam mène à l'hameçonnage. Mais nous devons réfléchir en effet à nos contrats à l'avenir.

Si l'on voit l'utilisation malveillante dans le rapport, il y a moins d'abus du DNS associés avec les nouveaux gTLD. Et on a peut-être connu certains succès avec les protections mises en place lors des nouveaux gTLD, lors des nouveaux contrats qui ont été signés donc. Il y a des pratiques nouvelles précises pour les opérateurs de registres, pour limiter donc ces utilisations malveillantes. Mais ça, c'est à renforcer à l'avenir.

ALAN GREENBERG : Merci beaucoup. Sébastien Bachollet.

SÉBASTIEN BACHOLLET : Donc je vais m'exprimer en anglais. Est-ce que vous avez fait des comparaisons avec les séries antérieures de gTLD ?

JONATHAN ZUCK : Pour quels aspects ?

SÉBASTIEN BACHOLLET : Pour tous les aspects. Est-ce que vous aviez des données des séries précédentes ? Parce que je ne sais pas si elles existent. Et qu'en avez-vous fait ? Quelle comparaison avez-vous effectuée avec les séries précédentes ?

JONATHAN ZUCK : Oui, Jordyn.

JORDYN BUCHANAN : Oui Sébastien. Ça dépend des sujets. S'il y a eu des données de collectées auparavant, il n'y a pas eu beaucoup de collectes de données au niveau de l'ICANN avant la préparation de cette révision. Donc entre 2000 et 2006, pas beaucoup de données collectées par l'ICANN. Pas beaucoup de chiffres.

Mais il y avait des parties tierces, des universités, qui ont fait des enquêtes. Et nous avons pris en compte ces enquêtes et ces enquêtes précédentes. Mais elles sont orientées principalement vers la concurrence. Par exemple, à quelle rapidité les TLD connaissaient une croissance – .biz, .info – dans les années 2000. Nous avons pu analyser leur rapidité de croissance.

On n'a pas vu beaucoup de différence dans la dynamique au niveau concurrentiel. Le grand changement, c'est que maintenant nous avons observé un ensemble beaucoup plus large. Avant, on comparait .biz et .com et maintenant nous avons collecté beaucoup plus de données. Nous avons comparé les gTLD historiques et la nouvelle série de gTLD, et comment ils s'établissaient au niveau concurrentiel. Mais on a fait le maximum pour trouver les données.

SÉBASTIEN BACHOLLET : Oui. J'aimerais ajouter quelque chose et c'est la dernière fois que je dirais cela.

Il a eu une collecte de données pour l'an 2000, pour la série de l'an 2000. Mais l'ICANN ne les a jamais publiés. Et lorsque vous avez parlé de parking, par exemple, ça a été fait ses études sur le parking. Ça a été fait. Des rapports ont été envoyés à l'ICANN là-dessus. Mais ils n'ont jamais été publiés. Et je crois que ça sera intéressant d'essayer de les trouver, ces rapports. Et si je suis le seul à le savoir, peut-être que les gens de l'ICANN peuvent me poser plus de questions.

ALAN GREENBERG : Donc très bien. Nous gérons bien notre temps. Nous avons eu deux de nos présentations. Excellentes présentations, j'aimerais vous remercier pour la qualité de cette présentation. Et nous allons maintenant avoir Dave Piscitello qui va se joindre à nous. Et vous allez voir dans l'ordre du jour qu'il va parler du TTFKAD. Donc c'est l'« Outil que l'on connaissait auparavant sous le nom de DART ». Donc vous n'avez pas le droit de cliquer vous-même. C'est d'autres personnes qui font avancer les transparents. Et on n'a pas non plus de laser. Je ne sais pas pourquoi, mais–

DAVE PISCITELLO : Eh bien, je vais me présenter. Je m'appelle Dave Piscitello. Je suis vice-président de la sécurité et de la coordination ICT à l'ICANN. Et avant que l'on mette à l'écran les diapositives, qu'est-ce que ça veut dire cet « Outil que l'on appelait autrefois DART » ? La plate-forme de rapport sur les abus de domaine. C'était un acronyme. L'acronyme DART.

Et avant d'arriver à Johannesburg, j'ai reçu un courriel de notre service juridique disant que l'ICANN avait reçu une lettre disant qu'il fallait cesser d'utiliser le nom DART parce que notre organisation à la marque de fabrique pour utiliser DART. Donc on ne peut plus parler de DART. C'est pour cela que l'on va parler d'autre chose.

Donc le projet maintenant, ça va s'appeler différemment. On va l'appeler DAAR, le projet des rapports d'activités malveillantes sur les domaines. Donc DAAR, ça veut dire maison en arabe. Ça a une signification en langue afrikaans également. Donc on ne parle plus de DART, on parle de DAAR. C'est noté. Et nous allons maintenant pouvoir commencer notre présentation et je vais me permettre de vous expliquer ce que nous avons fait.

Nous sommes en train de créer une plate-forme pour apporter les enregistrements de DNS au bureau d'enregistrement et aux registres de TLD. Nous avons fait cela pendant plusieurs années, depuis bien longtemps, avant que ce ne soit l'ICANN. Et quand

on écoute l'indignation de ceux qui sont ici concernant le nombre d'utilisations malveillantes, on voit qu'il y a très peu de données qui ont été présentées.

Les données viennent de sources commerciales et sont limitées ou viennent du secteur académique. Elles sont limitées. Et une des choses que nous avons décidé de faire était d'essayer d'être plus large et d'être aussi scientifique que possible dans notre approche. Donc nous avons étudié tous les registres de TLD, les bureaux d'enregistrement pour les données d'enregistrement. Cela veut dire que nous avons analysé plus de 2000 TLD. Nous avons regardé la littérature, les rapports commerciaux, et nous avons constaté que dans ces cas-là, on a un nombre limité de fournisseurs de données qui fournissent ces données. Nous avons un grand nombre de liens.

Et la plupart des efforts des CCT – nous voulons avoir des études historiques. Nous voulons pouvoir fournir des données en temps voulu. Mais nos données vont nous ramener pour tous ces TLD au 1er janvier 2017. Donc nous avançons. Nous avons une base de données très large pour les objectifs historiques. Bien sûr, le fait de collecter des données des TLD et des bureaux d'enregistrement va être facile. Et obtenir des données de réputation va être un peu plus difficile. Parce que beaucoup ne les gardent pas. Donc nous avons besoin d'un référentiel de ces données de réputation.

Nous étudions aussi les menaces multiples. Nous avons commencé par trois menaces identifiées par le GAC dans son avis. Il s'agit des réseaux zombies, des logiciels malveillants et de l'hameçonnage. Donc nous avons une autre attaque qui s'appelle le pharming, mais c'est une attaque de différents types.

Comme nous pensons que le spam est une partie importante ici du problème, le GAC, à Hyderabad, a correspondu avec le Conseil. Il a dit qu'il y a des exemples de menaces dans ce sens, comme on pouvait penser qu'on devait inclure le spam dans cette étude.

Ce que nous voulons faire, c'est créer une série de données, un ensemble de données qui ne soient pas biaisées, qui puissent être obtenus par différents secteurs en utilisant les mêmes moyens, que tout le monde puisse les réunir. Nous allons publier ensuite un rapport concernant la méthodologie utilisée. Ce que nous voulons faire, c'est mettre en place une pratique scientifique. Nous espérons que si nous continuons à travailler comme ça avec la méthodologie que nous utilisons, les résultats seront similaires à ce que nous avons trouvé jusqu'à maintenant.

Vous avez peut-être entendu parler de cette initiative de données ouvertes. C'est un projet d'activité qui se fait au niveau

du responsable de la technologie. Nous voulons accéder aux données que l'organisation d'ICANN et la communauté sont en train d'organiser. Donc ce que nous allons faire ici, avec ses données, nous espérons que nous allons pouvoir les publier.

Et l'utilisateur de ce projet va avoir des données en zone DNS. Des données WHOIS. Les données de réputation de sources ouvertes. Et certaines diffusions commerciales qui impliquent le paiement de frais.

Donc nous devons affronter certaines limites, certaines contraintes, dans le futur. Et c'est que nous aurons des données que nous pouvons utiliser d'une manière, parce que parfois nous ne pourrons pas partager ces données. Et à moins que l'on ait des accords au niveau des brevets. Mais si c'est ce que la communauté souhaite, nous pouvons analyser cette question.

Alors, quels sont nos objectifs ? Ce n'est pas ici un projet – un objectif de projet limité. Comme Greg l'a dit, au niveau des discussions, je serais ravi d'en parler moi-même. Identifier. Et si c'est la compagnie qui héberge le registre, le bureau d'enregistrement qui est responsable, ce n'est pas simple. Beaucoup de gens pensent que c'est beaucoup plus simple que ce que cela est en réalité. Trouver des actions à mettre en œuvre. Est-ce que cela dépend de la conformité ? Est-ce qu'il y a des actions qui doivent être mises en place dans une juridiction

par les forces de l'ordre ? Dans plusieurs juridictions ? C'est aussi quelque chose qui est difficile à gérer. Et je vous le dis, je le fais au quotidien. C'est un processus très complexe.

Ce que nous espérons pouvoir faire avec les données, c'est donner à la communauté des données qui sont dans le cadre du processus de politique. Parce que les politiques, parfois, nous n'avons pas assez de données pour que les gens puissent prendre des décisions. Donc avec ce projet de DAAR, nous voulons avancer, avoir davantage de données, permettre à la communauté d'accéder à ces données pour prendre des décisions informées sur cette politique et connaître leurs conséquences, etc. Donc c'est notre objectif.

Qu'est-ce qu'on peut faire avec ces données ? Nous espérons que nous pourrons identifier les menaces, voir quels sont les différents niveaux pour les TLD, si nous pouvons trouver les données. Ce serait bien, dans le futur, que nous puissions fournir une liste de menaces c'est quelque chose que nous voulons faire.

Nous voulons être capables de faire un suivi au niveau de la sécurité, des menaces qui existent. Parce que cela fluctue dans l'espace du DNS. On peut prendre TLD, par exemple, et il y a 60 jours ils avaient des enregistrements à 160 USD, et maintenant

ce prix a baissé. Donc il y a une grande variation sur la façon dont les enregistrements fonctionnent.

C'est la même chose pour le spam. Il y a différents types de femmes qui sont associées à des campagnes de messages massives. Donc une seule donnée ne nous aide pas.

Cependant l'histogramme, quand on l'analyse, ça nous donne un peu une idée de ce qui se passe. Et nous avons des données sur chacune de ses journées pour voir ce qui se passe, discuter avec un opérateur et lui dire qu'est-ce qui s'est passé ce jour-là précisément par exemple.

Donc nous pensons que cela va donner une opportunité au personnel d'ICANN pour travailler avec la communauté de l'ICANN, avec les parties contractuelles surtout, pour considérer les différentes manières de gérer ces données de réputation, les programmes d'utilisation malveillante. Et nous pensons que cela peut être très utile au niveau du service.

Il est clair que la partie la plus importante ici, les caractéristiques les plus importantes sont les comportements d'enregistrement malveillant. Parce que ça fait partie du système délictuel. Les gens enregistrent des domaines et les utilisent pour des actions délictuelles, et c'est un problème. Et comme Greg a dit cela, il apparaît que le nombre de domaines enregistrés de manière malveillante a augmenté. Donc c'est un

souci. Nous voulons comprendre comment cela fonctionne. Prochaine diapo ?

Voyons. Je vais vous expliquer un petit peu comment nous utilisons les domaines et les données. Nous collectons des fichiers de zone auprès des registres en utilisant les services centralisés ou les transferts historiques. Nous avons environ 195 millions de domaines. Nous avons tout cela dans un corpus avec 1241 TLD.

Et nous avons parlé à une série de ccTLD. Et j'ai fait cette présentation au symposium du DNS de Madrid. Plusieurs ccTLD sont venus me voir, voir comment il pouvait coopérer. Et cette semaine, à la ccNSO, j'en ai eu trois de plus. Ce serait très bien s'ils participaient tous, parce que nous aurons vraiment une idée très claire de l'espace des noms dans sa totalité.

Nous utilisons WHOIS, et heureusement, nous pouvons aborder tout le problème du GDPR. Parce qu'ici, ce qui concerne le WHOIS, c'est l'enregistrement. Donc c'est le portfolio du bureau d'enregistrement qui est concerné ici. Les données de contexte sont importantes. On peut trouver une utilisation pour la date de création, la date d'expiration, faire des analyses aussi de l'état minimum pendant lequel ce nom de domaine a été malveillant. Nous pouvons analyser les choses comme par exemple quand est-ce que ce domaine a d'abord été observé

dans le DNS. Mais nous n'avons pas besoin de choses liées aux informations d'identification personnelle.

Nous n'utilisons pas tous les noms dans un portefeuille de registres. Nous utilisons seulement certains. Et les menaces de sécurité peuvent être perpétrées contre les utilisateurs ou être exécutées si le nom ne peut pas être résolu à travers son adresse IP.

Et j'ai dit que nous utilisons beaucoup de séries de données de menaces. Nous avons consacré beaucoup de temps dans ce projet à essayer de décider quelle série de menaces nous allions incorporer et dont nous allions tenir compte. Nous avons 28 séries de données de 20 fournisseurs de réputation. Je peux vous dire qu'il y a beaucoup d'articles académiques commerciaux, de rapports qui ont été analysés. On a parlé avec les fournisseurs donc qui sauvegardent ces données pour comprendre leurs méthodologies et leurs pratiques.

Greg et moi-même, nous avons mis en place une liste et nous pensons que nous avons cette liste qui en général est exacte et qui nous donne une couverture mondiale et qui nous donne un taux assez positif.

Une des choses que nous voulons faire dans le cadre de ce projet, c'est que nous essayons de donner une idée de ce que la communauté des utilisateurs voit ou de ce que les entreprises

voient concernant le système de sécurité ou à travers un système de sécurité ou leurs mesures de défense qu'il mette en place pour se défendre contre ce type de mesure.

Nous essayons de prendre ces données et de voir comment d'autres communautés externes icône voient cet écosystème dans son ensemble. Et nous avons construit ce projet pour qu'il soit extensible. Et nous espérons que l'on pourra ajouter d'autres données une fois qu'on est sûrs que ces données sont fiables. Si on trouve que quelque chose peut être inclus dans cette liste, que ce que l'on utilise maintenant est moins valable ou moins exact, on peut le retirer aussi.

Et au niveau historique, une liste a commencé à être faite au niveau du projet de recherche. Il y a des financements qui ont été obtenus. Ce projet avance. Donc la réputation de la liste en elle-même fluctue en fonction des recherches que nous réalisons.

Je voudrais m'assurer que vous avez bien compris que l'ICANN ne crée pas actuellement des listes noires. Nous ne sommes pas en train de faire des recherches sur l'hameçonnage ou le spam ou autre. Nous utilisons le système de réputation que l'on nous fournit pour savoir quelles sont les URL des données abusives. Et nous essayons d'analyser les données que nous fournissent différents bureaux d'enregistrement. Nous classifiant ces

données en différentes catégories que j'ai déjà classées : le spam, l'hameçonnage, les programmes malveillants, l'hébergement, les réseaux zombies. Et nous avons donc un système qui nous permet de travailler pendant toute l'année à mesure que nous avançons et que nous avons accès à ces données.

Nous pouvons automatiquement aussi créer un histogramme. Nous faisons des tableaux qui comparent différents TLD, les nouveaux TLD par rapport au TLD historique et par rapport aux ccTLD, aux gTLD.

Lorsque nous comptons un domaine, nous avons des listes multiples. Des fois nous avons un domaine qui appartient à plusieurs listes. Donc nous essayons de corriger cela. Et des fois, nous avons l'impression d'avoir un ensemble assez exact des domaines qui sont responsables d'actions malveillantes. Voilà.

Ici vous voyez des données de réputation actuelle. Nous avons choisi cette liste pour nous assurer que nous avons au moins deux listes pour chacune des classifications de menaces concernant la sécurité, que nous analysons. Nous pensons que les mécanismes de classification sont cela, sont corrects.

Et nous avons reçu beaucoup de curiosité. Des fois, nous utilisons des séries de données et il y a beaucoup de doublons. Alors, pour faire davantage de recherche, lorsque nous parlons

avec certaines questions qui ont fait des recherches dans ce domaine, beaucoup de– il y a des gens qui ont fait des analyses de ce système de blocage qui ont constaté qu'il y a peu de listes de blocage et qu'il n'y a pas de doublons. La plupart des listes n'utilisent pas la même méthodologie ou ont des systèmes de collecte qui sont similaires, mais qui travaillent dans différentes zones géographiques, qui ont différents partenariats avec des fournisseurs de services différents.

Donc nous pensons que l'on peut utiliser avec confiance ces listes multiples. Et nous avons commencé avec une liste de 86 listes. Et le nombre de tests qui se font contraint son ensemble de TLD. Et on regarde les résultats de ces 86 listes qui confirment ce que ce document indique.

Donc je crois que cela représente ce qu'il y a de meilleur dans le secteur pour l'exactitude, la clarté. Nous utilisons cette classification lorsqu'on regarde les systèmes de sécurité au niveau des fournisseurs commerciaux. Nous avons aussi essayé d'évaluer la qualité en fonction de la littérature académique que nous avons consultée.

Alors je vais passer ici rapidement et répondre non à cette question. Nous ne tuerons pas toutes les actions malveillantes. Nous en capturant seulement quelques-unes et nous faisons une évaluation de ces actions.

Outre ce système que nous avons, un autre système sur lequel nous faisons des recherches actuellement, c'est une manière de mesurer les grands TLD comparés aux petits TLD. Et donc nous avons un pourcentage d'actions malveillantes, des mesures que nous voulons appliquer. Il s'agit de mesures qu'en général vous nous demandez d'appliquer et ça résulte des conversations que nous avons avec les SO et AC.

Un pourcentage d'abus assez simple à calculer, c'est une fraction, c'est le nombre de domaines qui étaient sur une liste d'actions malveillantes dans un TLD un jour donné, dans une série de domaines, à un moment donné dans une zone.

Le bureau d'enregistrement, c'est la même chose. Donc on a un nom de domaine divisé par le bureau d'enregistrement.

Je vais vous montrer ici certains échantillons. Ici vous voyez une visualisation des données que nous voulons partager. Ici, vous voyez le nombre d'actions malveillantes qui illustre le fait que l'hameçonnage et le problème du spamming semblent migrer vers les nouveaux gTLD ou sont distribués à travers tous les TLD, plutôt que– ne sont pas vraiment uniformes. Et les logiciels malveillants restent dans les TLD historiques plutôt. Donc voilà, ça, c'est une analyse dans une journée. Au niveau d'une journée.

Bien. Quelque chose d'intéressant. Il s'agit des données que nous avons explorées. Ici, vous voyez des points qui

représentent des domaines de TLD de premier niveau. Et les axes, vous voyez qu'il y a beaucoup d'axes. Parce qu'il y a une congestion à certains endroits, mais la ligne que vous voyez à travers les échelles qui représentent 0.6, qui est le taux moyen d'actions malveillantes. Et ce que vous voyez, il y a un grand nombre de TLD et de TLD historiques qui fait du bon travail, qui a de bons résultats. Et ce qui ne figure pas ici, sur cette diapo, c'est qu'au mois de mai, seulement une partie de ses TLD avec certains incidents. Donc il y a un nombre de TLD qui a eu ce type d'incidence.

Est l'endroit où on a une préoccupation, c'est au-dessus de cette ligne, l'axe qui dit « 10 ». Il y a 25 TLD qui ont eu un grand nombre de pourcentages d'actions malveillantes. Ils ont donc le plus grand nombre d'enregistrements malveillants ou d'actions malveillantes reportés dans le système.

Donc une interprétation de ce type de chiffre, de ce résultat, et pourquoi est-ce que cela arrive. Qu'est-ce qu'on doit faire en tant que communauté pour réduire cette quantité d'action malveillante et les amener à zéro.

Oui. J'ai presque terminé. C'est l'un des derniers transparents.

Donc où est-ce qu'on en est dans notre projet ? Nous sommes à la version bêta. Nous avons eu beaucoup de problèmes à collecter des WHOIS. Et nous avons été en mesure d'avoir un

meilleur mécanisme de collecte de données. Et c'est ce que nous gérons au quotidien. Nous avons donc – nous voulons que les opérateurs des ccTLD se joignent à nous. Et ce que je veux que vous reteniez, c'est qu'il faut trouver auprès de la communauté comment vous voulez faire des rapports sur ces informations. Quel type de représentation ou de résultats vous sont utiles et vous voulez que nous vous présentions ? À qui allons-nous présenter et quel accès aux données devons-nous prendre en compte ?

Donc je vais m'arrêter de parler et je vais répondre à vos questions. Merci beaucoup.

ALAN GREENBERG : Oui. Je vais devoir partir, donc je vais donner à Olivier. Olivier, vous pouvez gérer la séance ? Oui merci.

Donc il y a trois personnes qui veulent prendre la parole, et moi j'ai une première question puis nous aurons Alberto, Garth et ensuite Olivier prendra la parole. Il ne nous reste plus beaucoup de temps. Nous sommes en pause. Donc, revenez un petit peu en arrière sur le transparent – voilà. Oui. Oui.

Alors vous avez dit que vous n'êtes pas là pour faire honte à qui que ce soit. Mais là, on voit qu'il y a 100 % des problèmes dans

un [Inaudible]. Est-ce qu'on va voir les données qui vont nous permettre d'identifier qui pose ces problèmes ?

DAVE PISCITELLO : Donc ça, c'est une question pour la communauté. L'accès aux données. Moi je suis une base de données. J'ai une base de données pour vous. La communauté ICANN doit décider de la manière dont vous voulez qu'on représente ces données et sous quelle forme. Et il faut bien comprendre comment l'on bâtit cela, parce qu'on n'a pas d'interface pour utilisateurs où l'on puisse rentrer et taper les données, faire des demandes. Donc on va générer des systèmes de génération de rapports. Et on doit avoir une idée du type de rapport que vous voulez que nous vous fissions.

Et j'encourage l'ALAC à faire la même chose que le groupe de travail qui a présenté ces idées, et nous indiquer comment vous voulez avoir accès à ces données, quels rapports vous voulez que je vous fasse. Le GAC va faire la même chose. Donc si vous voulez connaître les noms, il faudra le justifier. Si c'est ce que vous voulez, je vous donnerai les données et vous générerez ces listes. Si vous voulez féliciter les gens parce qu'il y a des acteurs qui se voient très critiqués de manière anecdotique, et bien, ils sont parmi les meilleurs opérateurs du domaine. Donc je peux

vous créer une liste des meilleurs 25 bureaux d'enregistrement, des 25 meilleurs TLD. Tout est possible.

ALAN GREENBERG : Alberto, Garth. Moi je vais devoir vous quitter. Et les interprètes vont devoir vous quitter dans cinq minutes.

OLIVIER CRÉPIN-LEBLOND : Alberto Soto.

ALBERTO SOTO : Oui merci. Je vais m'exprimer en espagnol. Je sais que ce thème est très compliqué. Nous l'avons vu avec les exposés précédents. C'est aussi compliqué que prendre soin d'une personne âgée. En tout cas, ICANN doit s'occupait de cette personne âgée. Et cette unité constitutive est celle qui doit faire l'infirmière, le docteur, pour que cette personne âgée ne tombe pas gravement malade.

Donc ma question est la suivante. Le GAC, que va faire le GAC par rapport au premier objectif de ce projet ? Il s'agit de l'identification. Puisque l'ICANN ne peut pas travailler toute seule, donc Le GAC devrait s'engager à aider ICANN dans ce sens.

DAVE PISCITELLO : Oui merci. Eh bien, je ne vais pas parler au nom du GAC. Ce que je vous ai indiqué, c'est que j'ai présenté ces informations au

groupe de travail sur la sécurité publique, et il était très enthousiaste à ce sujet sur les possibilités qui s'ouvraient avec ces données. Et ils vont donc revoir ensemble cette liste de recommandations. Et au niveau du GAC, il aura une communication avec le Conseil d'administration et ils feront ce qu'ils voudront de cette liste.

Donc je ne sais pas ce que le GAC fera parce que, comme vous, je l'ai présenté en début de semaine. Je suis optimiste avec cet enthousiasme. Je crois que nous serons en mesure de faire d'excellents rapports.

OLIVIER CRÉPIN-LEBLOND : Merci. Moi j'ai une liste, grâce à mon prédécesseur, de Garth, Holly, Harold Arcos, Ricardo Holmquist. Et on a déjà dépassé notre temps imparti. Donc, Holly, Garth, vous voulez dire quelque chose ? Harold ? Vous pouvez parler par la suite.

DAVE PISCITELLO : Oui je peux rester.

OLIVIER CRÉPIN-LEBLOND : Ricardo aussi. Les interprètes n'ont pas eu de pause. Donc Garth Bruen.

GARTH BRUEN : Oui. ALAC, Amérique du Nord. Je voulais me faire l'écho de ce qu'avait dit Olivier tout à l'heure. On a entendu beaucoup de bruit et on n'a pas vu beaucoup d'action. Donc c'est très bien analysé les choses. Je n'ai aucun doute, Dave, que vos données et vos résultats vont être spécifiques et précis. Ça ne fait aucun doute. Je vous fais confiance. Le problème, c'est le suivi. Qu'est-ce qui va se passer par la suite de cela.

Assumons par exemple qu'il y a un processus qui permettra de faire respecter les règles. Peut-être que les prix vont augmenter. Peut-être que de nombreux noms vont être retirés du DNS pour utilisation malveillante. Peut-être qu'il y aura des mécanismes qui vont être créés pour, en effet, faire respecter ces critères. Ça va réduire les revenus de l'ICANN. Donc l'ICANN n'a pas grand intérêt financier à faire cela.

DAVE PISCITELLO : Oui. Vous savez, ça fait 15 ans que je travaille dans ce domaine. Et j'ai acheté à 50 USD un .com il y a très longtemps. Et je sais que les prix se sont écroulés. Et si ça était resté à 40 ou 50 USD, et bien, il y aurait bien moins de noms de domaines.

Donc je ne veux pas entrer dans des questions de tarification et de corrélation entre les prix et les problèmes. D'ici à Abu Dhabi, on pourra parler un petit peu plus. Mais il me semble qu'il est prématuré de faire des suppositions en disant que les revenus

de l'ICANN vont connaître des problèmes parce qu'on va ne plus avoir d'abus et limiter les abus.

L'utilisation malveillante utilise depuis toujours. Donc si on dispersa un peu les cafards, si j'ose m'exprimer ainsi, eh bien, peut-être que ce sera positif. Donc nous voyons qu'il y a des modifications. Il n'y a pas une grande augmentation de l'utilisation malveillante, mais il y a des modifications. Des tests qui sont faits par certains malfaiteurs qui passent d'un TLD à un autre. Et d'une manière « anecdotale », maintenant, on est passé de 100 à 50 je ne sais pas pourquoi. Mais il y a tant d'informations supplémentaires de surveillance qu'on peut effectuer avec ces données.

On doit avoir une meilleure compréhension des contre-mesures que l'on puisse mettre en place pour prévenir cela. Mais ça fait 12 ans que je suis ici, et pour le moment je crois qu'on a des données pour avancer et pour vraiment faire quelque chose de significatif pour gérer l'utilisation malveillante du DNS.

OLIVIER CRÉPIN-LEBLOND : Eh bien, merci beaucoup, Dave Piscitello. Une heure et demie d'un excellent programme, beaucoup de données qui ne sont pas toujours – qui ne portent pas beaucoup à l'optimisme pour les utilisateurs finaux. Merci à nos interprètes d'être restés un petit peu plus tard. Et je vais maintenant vous souhaiter une

bonne après-midi. On va aller à la séance principale qui se déroule dans les autres salles. Excellent après-midi. Je lève la séance. Merci.

[FIN DE LA TRANSCRIPTION]