SAN JUAN – Réunion du PSWG du GAC
Mardi 13 mars 2018 – 8h30 à 9h30 AST
ICANN61 | San Juan, Porto Rico

CATHRIN BAUER BULST : Bonjour à tous. Merci beaucoup d'être ici dans cette salle au lieu de rester à l'extérieur aux Caraïbes avec ce soleil et ce climat merveilleux. Donc merci énormément de vouloir consacrer ce temps à la réunion de travail sur la sécurité publique. Voilà donc la réunion officielle de ce groupe au sein du GAC.

Je m'appelle Cathrin Bauer Bulst et nous avons deux coprésidents. Je suis là avec Laureen Kapin.

Nous avons deux points à aborder dans l'ordre du jour. Nous allons parler du plan de travail du PSWG et puis nous allons parler du travail que nous faisons avec le bureau du directeur technique et ce que sont les outils du DAAR. Et nous allons permettre au reste des coprésidents de s'exprimer.

LAUREEN KAPIN : Moi, je fais partie de la Commission fédérale des États-Unis pour le commerce. Bien sûr, nous nous centrons surtout sur la protection des consommateurs et nous vous remercions d'être ici pendant la première séance du jour. Cette séance va durer de

8:30 à 9 :30. Vous allez entendre aussi dire : « Ah non, mais après 9 :30, vous allez continuer ? » Oui, c'est vrai parce que nous allons changer de sujet mais nous allons ensuite nous occuper de ce qui concerne le système du WHOIS et du RGPD, le règlement général de protection des données. Et nous avons un fort travail avec ce groupe de travail pendant la matinée. Donc j'espère que vous serez tous là pour la prochaine séance et j'espère que ce sera intéressant pour vous.

IRANGA KAHANGAMA : Bonjour. Je suis Iranga Kahangama. Je suis aussi basée à Washington avec le FBI. Et je vais travailler aussi. Et je vais parler de certains thèmes qui concernent l'usage malveillant du DNS et qui concernent aussi le DAAR. Nous allons voir quelques présentations et nous allons voir comment nous pouvons soutenir et mettre en œuvre les politiques, les recommandations ou faire des collaborations, collaborer de manière active dans cette initiative du DAAR. Nous croyons que cela sera très positif pour toute la communauté internet. Nous allons donc continuer à parler de tout ceci plus tard.

CATHRIN BAUER BULST : Merci beaucoup Laureen et Iranga. Laureen vient de me faire une suggestion intéressante. Pour ceux qui sont membres du groupe de travail sur la sécurité publique, je vous demande de

lever la main parce qu'il y a beaucoup de personnes du public qui s'intéressent à notre travail et qui, au fur et à mesure du déroulement de la journée, pourraient s'intéresser à nous contacter. Donc je demande aux gens faisant partie du groupe de lever la main pour que tout le monde vous reconnaisse et qu'ils sachent qui vous êtes.

LAUREEN KAPIN : Si vous avez des questions, il n'y a pas que ceux qui sont sur le podium mais il y a de nombreux membres qui sont tous disposés à répondre à vos questions.

CATHRIN BAUER BULST : Depuis la réunion de dimanche, vous savez que nous allons adopter le plan de travail pour la prochaine période de ce groupe de travail. Nous avons parlé de ceci d'une manière plus générale dimanche mais aujourd'hui, nous allons approfondir davantage notre commentaire si quelqu'un veut ajouter quelque chose pour le communiqué du GAC pour la fin de la réunion. Voilà, cela fait partie du plan de travail.

Le premier objectif stratégique se rapporte à l'atténuation de l'usage malveillant du DNS. Iranga a quelque chose à nous dire à propos de cela.

IRANGA KAHANAGAMA : Merci Cathrin. Comme je l'ai dit tout à l'heure, il s'agit de l'un de nos principaux plans de travail. L'objectif est de permettre à l'ICANN de trouver une meilleure position pour aborder cet usage malveillant du DNS. Il y a de nombreux rapports du [CCT] et c'est l'un des grands programmes qui sont en cours en ce moment.

Je vous demande d'aller sur la droite de l'écran. Comme je l'ai dit, il y a plusieurs projets sur l'information sur les activités concernant ces thèmes. Il y a aussi l'indice de santé du GTLD. Tout ce qui concerne l'initiative des données ouvertes de l'ICANN, tout cela concerne le fait de chiffrer cet abus, cette santé au niveau macro. Nous serons donc en meilleure position de vous informer sur ces usages malveillants.

Nous sommes en train de créer des principes. L'idée est d'avoir une ligne de base pour comprendre certains mécanismes génériques qui pourront être acceptés par toutes les parties de la communauté. Nous pouvons donc nous mettre tous d'accord là dessus. Il faut que nous nous mettions tous d'accord en tant que groupe.

Et en ce qui concerne le travail plus récent, l'un des thèmes que nous avons abordés est celui du SSAC. Ils ont plusieurs initiatives intéressantes auxquelles nous voudrions participer de manière formelle. Je crois que pendant cette réunion, il y a une

séance à 15:15 demain. C'est une réunion ouverte. Tout le monde peut y assister d'après ce qu'on nous a dit. Donc ce serait intéressant de voir dans cette réunion certains aspects de sécurité sur lesquels ils travaillent, les services d'enregistrement et les aspects techniques qui concernent tout cela. C'est très important par suite des considérations liées au RGPD.

Il y a des gens qui sont vraiment axés sur la sécurité. L'idée serait donc d'établir des rapports plus formels avec eux pour que nous puissions avoir des échanges. Il s'agit donc de ce sur quoi nous essayons de travailler. Il y a plusieurs sujets qui sont fondamentaux et qui se rapportent à l'usage malveillant du DNS. Ce thème est aussi un thème vraiment prioritaire.

CATHRIN BAUER BULST : Avant que Laureen n'aborde le troisième point concernant la protection des consommateurs, je veux rappeler aux membres du GAC que vous avez une copie de ce groupe de travail comme une annexe des documents qui vous ont été présentés en tant qu'annexe du point 11 débattu dimanche dans notre ordre du jour. Donc vous pouvez aller voir ce plan dans cette annexe.

LAUREEN KAPIN : Pour ce qui est des mesures de protection de consommateurs, ce thème a été très important pour l'équipe de révision sur la

confiance, le choix et la compétition pour les consommateurs. Ce thème est une suite du travail déjà entamé, à savoir lutter ou se battre pour des politiques pouvant protéger le public en ligne. C'est l'objectif le plus général et le plus important de cette partie de notre travail. Nous participons à différentes révisions pertinentes.

Aussi, nous avons établi une coordination avec différentes parties de l'ICANN ainsi qu'avec la communauté pour parler de ces thèmes parce que tout le monde s'intéresse à conserver quelque chose qui soit sûr pour les consommateurs et que les consommateurs nous fassent confiance pour continuer à se servir du DNS. Il y a différentes parties prenantes dans différents domaines du travail, y compris ce que sont les procédures ultérieures à l'introduction des nouveaux gTLD ainsi que le PDP, ce qui concerne l'accréditation des services d'anonymisation et de représentation, d'enregistrement fiduciaire.

CATHRIN BAUER BULST : Bon. Je vais parler des points suivants, des points d'actualité qui sont sur la page suivante et qui se rapportent à l'usage malveillant du DNS.

Lorsque nous parlons de responsabilité, cela signifie que nous cherchons quelqu'un qui s'occupe de travailler sur ce point. Il y a différents domaines qui se rapportent à la sécurité publique et

qui sont pertinents pour le GAC et pour le groupe de travail sur la sécurité publique. Ce que nous voulons, c'est améliorer notre capacité parce que nous sommes très peu nombreux à prendre en charge ce travail. Donc s'il y a quelqu'un qui veut participer dans un aspect important ou intéressant, nous vous demandons de venir nous voir après cette réunion.

LAUREEN KAPIN : Oui, c'est juste là ou nous vous demandons de nous aider à vous aider.

CATHRIN BAUER BULST : Par rapport à la sécurité, nous en parlerons de façon plus détaillée pendant la deuxième demi-heure de cette réunion parce que comme on le disait tout à l'heure, nous essayons de trouver des sources de données nous aidant à évaluer la politique existante de manière plus fiable ainsi que pour pouvoir faire les choix pertinents pour les nouvelles politiques, c'est-à-dire tout mouvement ou toute série ultérieure pour les nouveaux gTLD. Il faut donc que nous disposions de sources de données correctes disponibles pour être mieux à même de prendre des décisions quand il le faudra.

Ensuite, nous allons parler de la manière d'éviter l'exploitation du DNS pour éviter un usage malveillant. Nous allons nous

centrer sur les différents usages malveillants et nous allons bénéficier de l'interaction avec le SSAC.

Et du côté de la politique, nous allons voir comment nous pouvons travailler de manière plus efficace pour éviter ceci. Ce travail inclut une piste de travail concernant la lutte sur l'usage malveillant envers les enfants et nous voulons surtout voir ce qui se passe par rapport à l'efficacité des mesures de protection que le GAC a proposé pour protéger surtout les enfants sur des sites qui sont associés à certaines choses comme la confiance qui peut être liée par rapport à .kids, c'est-à-dire enfant. Il y a des attentes légitimes de la part des utilisateurs en ce sens qu'il s'agit de sites sûrs pour les enfants. En prenant des mesures liées au communiqué de Beijing, il faudrait adapter tout cela pour les prochaines séries de nouveaux gTLD. Il y a une piste de travail et je ne veux pas parler beaucoup plus. C'est le domaine dont je veux parler. Je sais que l'équipe italienne du GAC s'est vraiment centrée sur ces thèmes.

Avant de clore cette intervention, je voudrais savoir si vous avez des commentaires ou des questions.

Nous allons donc aborder le projet objectif stratégique centré sur le RDS en particulier. Cela concerne le WHOIS et l'accès aux données d'enregistrement.

LAUREEN KAPIN : Comme je vous l'ai dit, je vais diviser tout cela parce que nous allons en parler de manière approfondie après la pause-café. C'est juste pour que vous sachiez que le système du WHOIS et tous les bénéfices et les responsabilités y afférentes font partie de notre piste de travail et nous nous sommes entrés sur cela pendant cette dernière partie de notre travail.

CATHRIN BAUER BULST : Cela nous amène donc à la considération du PDP de nouvelle génération. C'est quelque chose qui est encore en marche.

Il y a ensuite l'exactitude des données d'enregistrement. Vous savez qu'on en parle depuis longtemps. Il y a aussi une mise en œuvre pour vérifier la syntaxe dans l'exactitude de l'enregistrement des données.

Ce que la communauté n'a pas encore abordé, c'est la question de l'identification des titulaires des noms de domaine. Il y a toujours, au point de vue de la sécurité publique, il y a de nombreuses possibilités d'améliorer la qualité de ceci, surtout pour ce qui est des données d'enregistrement du RGPD. Dans le monde des ccTLD, je crois qu'il y a encore des possibilités à ce que ceci soit plus fiable sans que ce soit plus coûteux. Nous allons voir donc comment ces efforts peuvent être transposés dans le monde des gTLD.

IRANGA KAHANGAMA : Je veux ajouter quelque chose. Cette section est très importante parce qu'il faut que nous pensions que le RGPD exige aussi une exactitude des données et cela fait partie de notre responsabilité. Il faut que nous en soyons... Nous pouvons avoir les données et leur accès mais il y a cette deuxième partie, à savoir vérifier l'exactitude de ces données dont nous disposons. Il faut que nous soyons conscients de cela parce que ce sera un outil très important et ce sera quelque chose qui devra être incorporé pour la prochaine version du WHOIS parce que ce sont les conditions ou les exigences du RGPD.

CATHRIN BAUER BULST : Merci Iranga. Le dernier point pour ce deuxième objectif stratégique concerne la mise en œuvre, à savoir quel est le respect ou la réalisation de la mission de l'ICANN par rapport au RDS. Ce qui est important ici, c'est que nous avons une équipe de révision et on a nommé la représentante des États-Unis, de l'INTERPOL et moi-même ; nous avons été désignés pour y participer. Il faut que nous voyions ce qui a se passer lorsque nous nous retrouverons pour la réunion de Panama.

LAUREEN KAPIN : Bien. Voilà donc l'objectif stratégique numéro 2. Est-ce que quelqu'un a des commentaires sur ces points qui sont inclus dans nos objectifs spécifiques ? Bon.

Nous allons aborder l'objectif stratégique 3, à savoir les fondements et la génération d'une opération flexible et efficace sur PSWG. Ceci concerne notre cadre d'organisation et nos procédures. Vous allez voir donc que nous parlons ici du développement d'un plan de travail ; c'est le premier pas. Il y a ensuite le renforcement du leadership comme on l'a dit dimanche. Nous voulons avoir un grand référentiel, pour ainsi dire, parce qu'il y a de nombreux thèmes importants et nous voulons que les gens se centrent sur ces différents points.

Nous voulons aussi augmenter le nombre de membres qui sont avec nous. L'une de nos idées a été de parler avec tous les membres du GAC. Et cela nous encourage de savoir que tous les membres du GAC ont considéré l'idée de désigner quelqu'un et de diffuser et de se mettre en contact avec les autorité d'application et les experts en sécurité publique de leur gouvernement parce que dans chacun de vos pays, vous avez des experts sur ce qu'est la recherche, sur le front disons, et comment savoir et comment détecter des activités criminelles, surtout lorsque nous parlons du DNS.

Nous savons que ceci devient parfois trop technique, trop complexe. Et dans chaque pays, vous avez des experts que vous pouvez consulter. Alors nous vous encourageons à le faire de manière formelle, à les contacter, à les désigner en tant que conseillers du groupe de travail de la sécurité publique, à leur permettre de participer dans les appels ou dans la liste de diffusion. Donc il est très important que tout le monde participe de manière active sur toutes ces questions concernant la sécurité publique. Je voulais donc souligner ce point.

Bien sûr, nous sommes un comité consultatif du comité consultatif gouvernemental et nous devons nous assurer que nous avons une communication de manière cohérente avec le GAC, avec ses autorités pour que l'on sache sur quoi nous travaillons. Nous allons vous faire savoir s'il y a un thème d'actualité qui demande votre attention et une résolution rapide de votre part.

Nous avons eu un exemple récent de cela il y a peu de temps parce que nous vous avions demandé d'analyser des points très complexes. Nous vous avions demandé de le faire très rapidement. Ce n'est pas la situation idéale mais malheureusement, c'est la situation où nous nous trouvons. Nous voulions donc nous assurer que nous faisions tout ce qui était possible avec la plus grande efficacité possible, vous mettre au courant de ce qui se passe, vous donner l'alerte pour

que vous révisiez quelque chose qui se rapporte au PSWG et recevoir vos commentaires pour pourvoir travailler avec vous et pour que le produit final reflète vraiment une position de consensus du GAC. Voilà notre plan.

À cet égard, nous sommes toujours attentifs au fait que nous voulons écouter ce que nous faisons correctement et ce que nous pouvons améliorer. Ne soyez pas timide. Nous voulons parler avec vous dans les couloirs, au téléphone. Chaque fois que vous estimerez qu'il faut faire des ajustements ou des modifications, nous sommes là pour vous écouter. Voilà donc l'objectif stratégique 3 de notre plan de travail.

Je voudrais donc des commentaires ou des questions à cet égard. Jason.

JASON : Bonjour, je m'appelle Jason. Je suis membre du PSWG pour représenter le Canada. À Abu Dhabi, on a dit qu'il s'agissait d'un groupe relativement homogène en ce sens qu'il y avait de nombreux membres de l'Amérique du Nord et de l'Europe occidentale. Mais je voudrais dire que nous aimerions diversifier la composition de notre groupe. Si vous avez des personnes dont vous estimez qu'ils pourraient être des candidats appropriés pour travailler avec ce groupe sur la sécurité publique, venez nous voir. Nous pouvons vous dire comment le

faire, comment y participer. Plus la diversité sera grande, plus nous serons forts. Voilà le message que nous voulons transmettre. Le fait que nous soyons nombreux à venir de l'Amérique du Nord ou de l'Europe occidentale, cela ne signifie pas que nous ne voulions pas avoir les opinions des membres des autres parties du monde. Venez nous voir et nous pouvons vous aider à rejoindre notre groupe, à travailler avec nous ou que quelqu'un parmi les autorités de la sécurité publique se rapproche de nous.

CATHRIN BAUER BULST : Merci d'avoir signalé ceci. C'est très important. Je veux ajouter que plus grande est la diversité, plus on pourra refléter la composition du GAC. C'est très important pour nous puisque nous sommes un groupe de travail qui vous aide à faire votre travail. Et on fonctionnerait mieux si on pouvait refléter les différentes positions ou points de vue du GAC.

Une grande partie de notre travail n'est pas faite au cours de ces réunions. Nous avons des téléconférences mensuelles, des appels mensuels, aussi hebdomadaires parmi les responsables des quelques questions en particulier. Normalement, on le fait à travers Adobe Connect. Et si vous voulez désigner un expert ne pouvant pas assister aux réunions, c'est mieux si vous pouvez participer aux réunions en personne de temps en temps. Mais la

plupart du travail est fait en dehors des réunions, à partir de la participation à distance. Je vous encourage donc à investir du temps dans le travail de ce groupe. Le fait de ne pas pouvoir être présent ne va pas vous empêcher de pouvoir collaborer. Il y a d'autres commentaires sur ce point 3 ? Ou si vous voulez vous incorporer, freinez votre enthousiasme.

S'il n'y a plus de commentaires à cet égard, on va passer à notre objectif stratégique 4 qui a trait à la diffusion externe, à prendre contact avec d'autres parties intéressées en dehors de cet environnement. Nous évaluons ce que nous faisons dans notre plan de travail et l'un de points principaux, c'est de nous assurer que lors de établissements des priorités, que ces priorités soient correctes. Pour savoir cela, il faut établir une communication pour savoir ce qui vous affecte dans les politiques qui sont en cours, comment fonctionne la mise en œuvre des politiques actuelles, quelles sont les possibilités d'amélioration, quels sont les problèmes qui apparaissent que notre groupe devrait traiter ou bien que notre groupe puissent en informer le GAC.

Nous travaillons également pour développer la prise de conscience de notre groupe de la part des organismes intergouvernementaux pour que les différents pays soient au courant que nous sommes ici, que nous pouvons aider. Il ne s'agit pas seulement de la politique. Il y a aussi la sécurité publique qui peut se refléter dans notre travail.

Nous travaillons aussi pour éliminer les barrières à la participation, c'est-à-dire on essaie de donner de meilleures informations. Peut-être vous êtes familiarisé avec tout cela. Lorsque l'on explique ce que l'on fait à l'ICANN, les gens ou bien ils s'endorment ou bien ils disent « Le temps est fini. » Alors c'est vraiment difficile de pouvoir obtenir l'aide nécessaire. On se dit « Que va t-on faire ? » On en parle mais cela nous prend beaucoup de temps d'arriver à une conclusion. C'est pour différentes raisons qu'il y a des difficultés. Il faut comprendre l'importance de ce que l'on discute ici et que cette personne s'informe comment contribuer à la discussion. Nous travaillons pour réduire ces barrières à partir des bulletins d'information, des résumés pour que notre travail soit plus accessible pour ceux qui ne le connaissent pas profondément.

On a eu de très bonnes collaborations au cours de nos réunions pendant la période intersession parce qu'il y a des organismes qui ne participent pas à ce travail et qui nous ont posés de très bonnes questions pour savoir pourquoi on travaillait sur X chose. Ils nous ont partagé leurs idées. Nous travaillons pour mettre en œuvre ces idées. Et comme vous pouvez le voir, il y a l'espace pour plus de bénévoles. C'est comme si j'essayais de collecter des fonds ici.

IRANGA KAHANGAMA : Merci Cathrin. C'est peut-être le site approprié pour mentionner que nous espérons parler avec le SSAC en plus grande profondeur pour vous expliquer ce que nous faisons. Leur travail est très intéressant aussi. Et au cours de nos activités, nous avons parlé avec les registres et les bureaux d'enregistrement sur les questions ayant trait au RDS, au WHOIS pour savoir quel est leur point de vue sur le développement de tous ces débats. Voilà donc la diffusion externe que nous faisons.

OCTO, c'est bien évident, on va l'aborder dans quelques instants. Et il y a beaucoup de créativité dans ce domaine. Alors si vous avez des idées de communautés qui puissent être intéressées, dites-le nous.

CATHRIN BAUER BULST : Merci. Il y a un évènement social que nous avons ce soir avec les bureaux d'enregistrement à 18:30 à la terrasse. Rejoignez-nous s'il vous plaît pour connaître la question et d'autres membres de la communauté. Je ne sais pas s'il y a une autre idée ou si quelqu'un veut prendre la parole ?

Autrement, nous finissons la révision du plan de travail. Si vous avez des commentaires, des questions ou des suggestions, et bien rejoignez-nous, envoyez-nous un courriel aujourd'hui, sinon nous transmettrons cela au GAC pour qu'il sache que le plan de travail est passé pour approbation.

Cela veut dire que nous pouvons passer à la deuxième partie de notre réunion ayant trait à la conversation sur OCTO et DARR. Je vois que David s'approche du podium. Merci d'être ici pour que nous puissions mieux comprendre la question. Je sais que tu es très enrhumé et je le regrette.

DAVID CONRAD : Bonjour à tous. Je m'excuse de ma voix, je suis très enrhumé. Peut-être je vais tousser un tout petit peu. Je remplace John qui semblerait avoir un bon temps après le gala.

Nous passons donc à la diapositive suivante. Je suis certain que la plupart parmi vous, vous êtes familiarisés avec le DAAR. Le DAAR est un système d'informations que nous développons avec l'aide du groupe des menaces cybernétiques pour identifier l'utilisation malveillante, l'abus, notamment les instances identifiés par le GAC dans leur communiqué de Beijing, qui a trait au pharming et au spam.

Quelle est la différence entre DAAR et d'autres outils qui sont disponibles ? Et bien par la quantité de données que nous collections, on a différents courants de données cumulées et ces données sont collectées et stockées pour pouvoir faires des études historiques. Nous allons nous focaliser dans la multiplicité de type d'abus que nous pouvons repérer là où on crée des informations transparentes et reproductibles pour

faciliter la communication et ainsi développer des politiques au sein de la communauté de l'ICANN.

J'en ai déjà parlé. Ce qui est important de signaler dans ce cas, c'est que nous donnons des licences à une grande partie des données que nous utilisons pour DAAR et dans certains cas, elles ne sont pas disponibles.

Pourquoi peut on utiliser ce système DAAR ? L'objectif principal est de pouvoir informer les activités qui représentent une menace au niveau des bureaux d'enregistrement. On peut l'utiliser pour faire des études sur la menace à la sécurité. Aussi, il peut aider aux opérateurs, aux bureaux d'enregistrement, aux opérateurs de back end à comprendre ou considérer comment ils peuvent gérer leur réputation dans leur système anti-abus. Cela nous permet aussi de faire une étude des conduites d'enregistrement malveillantes et aussi pour aider les communautés de sécurité opérationnelle.

Un des ensembles de données que nous utilisons, ce sont les données des zones TLD. On collecte toutes les données de zone TLD pour analyser les registres de gTLD. On utilise le service centralisé de données de zone. Et le DAAR utilisera seulement les domaines qui apparaissent dans la zone. On ne va pas essayer de chercher les bases de données des registres ou des bureaux d'enregistrement avant que ces noms soient inclus dans des

zones. Actuellement, on a quelque 1240 gTLD, ce qui nous amènent à 185 millions de domaines environ. Plusieurs ccTLD nous ont rejoint pour participer à l'initiative DAAR et il faut voir comment les incorporer à notre système DAAR.

DAAR utilise également le WHOIS. On utilise une petite portion du WHOIS, notamment les données des bureaux d'enregistrement. Mais cela peut être assez problématique étant donné que DAAR est focalisé pour essayer de trouver un système reproductible. Alors on ne génère pas d'informations disponibles en interne au sein de l'ICANN. Nous utilisons des informations qui sont disponibles au public. En conséquence, nous essayons d'obtenir des informations pour des millions de domaines à travers les serveurs de WHOIS existants. Et comme vous le savez, ceci peut être ou peut représenter un véritable enjeu, du point de vue de la vitesse notamment.

Si nous voyons les ensembles de données de menace, nous en utilisons plusieurs. Nous essayons d'identifier les données pour qu'il n'y ait pas de faux positifs. Nous utilisons les ensembles de données d'abus d'URL ou de domaines multiples pour pouvoir en réalité voir ce qui est associé au hameçonnage, le malware, le phishing bottom et le spam. Et puis, nous essayons de créer des histographies, des tableaux et des graphiques dans le but de refléter comment ceux qui sont en dehors de la communauté de l'ICANN voient l'écosystème des noms de domaine.

Dans cette diapositive, vous voyez qu'à OCTO, nous ne préparons pas nos propres listes. Nous présentons un cumulé des données disponibles à travers des entités externes. Ces entités génèrent ces listes qui bloquent les menaces. DAAR collecte les données d'abus qui sont informées à l'industrie. Donc on ne crée rien de tout neuf ici. Une des inquiétudes communes, c'est que nous générons de nouvelles données qui ne sont peut-être pas exactes mais dans de nombreuses opportunités, on a réitéré que c'est ce que les opérateurs de courriers utilisent au quotidien. On ne crée rien de tout neuf.

Les critères pour inclure ces listes de blocage de réputation dans le système doivent être classés par rapport aux menaces qui soient cohérentes avec nos propres menaces à la sécurité. Ces communautés de sécurité doivent se fier de ces listes. Pour mener à bien le processus, il faut qu'il y ait des réputations positives et ces listes doivent être pleinement acceptées au sein de communautés de la sécurité opérationnelle. Cela est démontré à travers le fait que ces données sont incorporées aux systèmes de sécurité commerciaux et aux produits commerciaux qui sont utilisés par les opérateurs de réseau pour protéger leurs utilisateurs et dispositifs et qui sont également utilisés par les fournisseurs de courrier électronique pour protéger leurs utilisateurs du spam et d'autres attaques.

Les RBL bloquent le courrier électronique non demandé, c'est-à-dire le spam. On utilise une liste d'APWG et il y a des systèmes de nuage aussi, par exemple Amazon utilise un autre système. WAF utilise ces listes pour bloquer les abus, les attaques volumétriques et les RBL bloquent les URL malicieux. Nous avons aussi des RBL dans le DNS qui utilisent les zones dans le résolveur, etc. Plus de détails sur les listes de blocage.

Nous utilisons aussi des questions qui ne sont pas expérimentales. C'est quelque chose qui est utilisé dans les services commerciaux, dans la production.

Nous avons également travaillé avec les études académiques pour réviser l'information et les pratiques utilisées pour voir comment les chercheurs peuvent arriver à une information fiable. Il y a une série d'études et de rapports que nous utilisons pour DAAR.

Alors l'ensemble de données RBL que nous utilisons maintenant sont les listes de domaine SURBL et aussi la liste bocage de domaine, spam house, la liste anti hameçonnage. Voilà. Il y a toute une liste de ce que l'on utilise pour identifier les logiciels malveillants.

DAAR n'identifie pas tous les types d'abus. Il n'y a aucun fournisseur ayant une réputation qui puisse avoir tous les abus. Chacun a son propre point de vue. Différents RBL sont focalisés

dans différentes choses spécifiques et voilà pourquoi nous faisons cette cumulation de tous les RBL ; parce que nous voulons avoir une liste intégrée de tout ce que l'on voit sur internet.

Normalement, nous recevons une question parce que nous informons les domaines qui sont du spam. Le GAC a manifesté son intérêt d'avoir des informations sur l'utilisation du spam. Et de notre point de vue, la plupart du spam est envoyé travers des moyens doublés ou illégaux à partie de réseaux zombie. On ne l'associe pas au contenu du courriel électronique. Il y a du spam à travers les Twit, aussi à Facebook et dans d'autres systèmes de messagerie et en fait, le spam est un des principaux moyens à travers lesquels on met en place d'autres menaces mentionnées dans le communiqué du GAC de Beijing. Alors on voit cela comme un service dans le nuage, par exemple le réseau zombie d'avalanche, il a donné des enregistrements de domaines à ses clients pour faciliter la transmission de spam.

DAAR, ou ce que nous utilisons à DAAR, sont les noms de domaine que l'on trouve dans le corp des messages de spam, là où les gens cliquent pour pouvoir déclencher la décharge d'un logiciel malveillant ou des choses de la sorte. Ce qui est important, c'est que la réputation du domaine de spam influe sur la manière agressive ou non que l'on applique les filtres. Les administrateurs des systèmes se focalisent tout d'abord sur le

spam parce que c'est un très bon indicateur des domaines concernés.

Maintenant, dans le système DAAR qui en est déjà à son étape d'exploitation, nous l'utilisons en interne depuis longtemps. Nous n'avons pas publié de rapport généra par le DAAR parce que nous voulons travailler comme il le faut. Nous ne voulons pas travailler rapidement. Ce que nous avons, c'est une révision d'un tiers indépendant par rapport à la méthodologie du DAAR pour compiler les données, pour recueillir les données. Et ces révisions dont l'une d'elles s'est terminée hier, la deuxième se terminera d'ici deux jours à peu près, et nous allons donc présenter ces rapports à la communauté. Si les rapports présentent des suggestions de modification, bien sûr, nous allons mettre en œuvre ces modifications. Notre intention est que ces révisions nous aident à aider le SSAC pour que le SSAC nous dise comment nous devons travailler avec la méthodologie utilisée par DAAR.

En ce moment, les rapports internes, ces graphiques nous avons là, n'ont qu'un caractère interne. Notre objectif en ce moment est de les rendre accessibles à la communauté pour qu'ils puissent parler en termes de politiques sur ce qui concerne l'usage malveillant du DNS. Vous pouvez voir que tous les gTLD ont au moins un nom de domaine où l'on a enregistré un usage malveillant. Vous voyez qu'il y a différentes couleurs pour voir

comment cet usage malveillant a été signalé et comment il a varié avec le temps. Il est évident que le spam est le plus populaire disons, mais il y a aussi le pharming et le phishing.

Au sein d'OCTO, nous avons pris cette information créée par le DAAR et nous faisons ces graphiques de bulles. Si nous avions des animations, vous pourriez voir comment ces bulles grandissent. Comme on le voit là, ce n'est pas très intéressant. Donc ce que l'on peut voir ici, c'est que les domaines ayant du phishing ou du hameçonnage sont les plus importants en général. Il s'agit des domaines les plus grands. Mais c'est une tranche relativement limitée.

Nous avons commencé à voir des choses qui s'écartent du royaume de la statistique normale, disons. Ce que nous allons faire, c'est publier les noms pour que l'on ait une idée des registres et des bureaux d'enregistrement qui sont les plus soumis ou qui sont les plus souvent soumis à l'usage malveillant que les autres. Clairement le spam est quelque chose d'intéressant qui est variable avec le temps. Vous pouvez voir ces bulles qui vont de gauche à droite et qui montent et qui descendent. Et il est très intéressant de voir ceci parce que cela nous met au courant de ce que nous appelons le flocking, ce qui signifie passer dans un grand groupe d'un bureau d'enregistrement à un autre groupe d'enregistrement. C'est ce que nous appelons le flocking.

Voilà entre les gTLD et les gTLD historiques, nous voyons que les gTLD historiques ont des chiffres connus. Et nous voyons aussi qu'il en va de même pour les nouveaux gTLD en ce qui concerne l'enregistrement. Et il se peut que ce soit un usage malveillant.

Là, nous voyons l'usage malveillant des domaines figurant sur le DAAR, sur le système de signalement des cas d'utilisation malveillante des noms de domaine. Et il y a une utilisation dans les nouveaux gTLD. L'une des caractéristiques du DAAR, si vous vous intéressez à l'usage malveillant, c'est que vous pouvez en obtenir un bon nombre données qui vous font savoir ce qui se passe là, c'est-à-dire c'est ce qui occupe mon équipe. C'est pour cela que nous nous centrons sur la prévention de cet usage malveillant.

Nous avons ici ces statistiques qui nous montrent qu'il y a un nombre relativement petit de domaines qui sont ceux sur lesquels se centrent le plus grand nombre des usages malveillants. C'est quelque chose que nous savons depuis un certain temps, mais DAAR nous fournit des données concrètes à cet égard.

Voilà l'état du projet. Comme je l'ai dit, nous nous centrons sur quelque chose de bien fait et non pas sur quelque chose qui soit fait à la va-vite. Comme je l'ai dit, nous avons des rapports des réviseurs. C'est quelque chose que nous allons vous présenter

cette semaine. Nous ajustons le système de collecte de données pour créer des mises à jour qui soient flexibles et opportunes. L'idée est de pouvoir enfin automatiser une bonne partie de ce rapport pour ne pas avoir de main d'œuvre manuelle et de faire tout cela de manière automatique. Nous allons voir comment nous faisons la distribution granulaire de tout cela et nous faisons des expériences avec des mesures supplémentaires. Voilà, nous avons fini, donc, sur ce point.

Il y a un domaine qui est le plus complexe, concernant la collecte de l'information sur les bureaux d'enregistrement et cela se rapporte au WHOIS. Et maintenant, nous ne sentons pas que les données de ces bureaux soient trop fiables. Il se peut que nous puissions plus tard le faire mais nous avons besoin de réfléchir un tout petit peu sur la manière dont nous pouvons recueillir les données des bureaux d'enregistrement et que ce soit efficace.

Je finis sur cela et je cède la parole à Fabien, à moins qu'il n'y ait des questions.

LAUREEN KAPLIN : Merci beaucoup de cette présentation, Dave. Nous sommes très reconnaissants à l'ICANN de l'effort qu'elle fait. Cette information sera cruciale pour nous, surtout pour ce qui concerne le développement de politiques parce que cela met

sous la loupe quels sont les problèmes, l'attention que nous devons y accorder lors de l'élaboration des politiques, s'il faut changer les procédures, s'il faut les modifier pour avoir une manière de combattre cet abus ou cet usage malveillant systémique qui se produit. Nous voudrions donc savoir ce que l'on pourrait faire avant que cette initiative ne soit en usage public pour voir si cela se trouve dans les registres, les bureaux d'enregistrement, etc.

DAVID CONRAD : Comme je l'ai dit, notre priorité avant la publication des noms liés aux données que vous pouvez voir là, il s'agit donc d'avoir une révision d'un tiers pour vérifier que nous ne commettons pas d'erreur avec les données pour minimiser les possibilités d'avoir des faux rapports ou qu'il y ait une mauvaise attribution pour tout ce qui concerne le DNS et essayer de donner un certain niveau de confiance à la communauté dans ce sens où les données que nous utilisons puissent être utilisées pour obtenir de l'information concrète basée sur des données concrètes pour nous occuper de l'élaboration de politiques. Lorsque les réviseurs indépendants auront fini leur travail, on va finir et je crois que dans quelques jours, ils vont finir. Nous pourrons donc présenter ces rapports et nous pourrons commencer le processus concernant la rédaction des rapports pour pouvoir les présenter à la communauté et indiquer de la

sorte quelles sont les statistiques réelles et quels sont les acteurs dans ces statistiques.

CATHRIN BAUER BULST : On a parlé du rate limiting. Mais je ne suis pas sûre si j'ai bien compris ce que cela signifie.

DAVID CONRAD : Dans les services de réseau, on peut avoir un déni de service pour commencer une collecte de données plus vite que ne peut le faire le système. Les opérateurs des réseaux de service imposent une limitation pour réduire le nombre de connexions qui peuvent s'établir pour éviter l'utilisation malveillante. Dans le contexte des registres et des bureaux d'enregistrement, à vrai dire, je crois qu'ils ont tous cette limitation de vitesse, et alors les gens ne peuvent pas aller chercher sur toutes les bases de données pour chercher les contacts ou créer des messages spam. L'effet collatéral est que les chercheurs essaient de collecter cette information pour attribuer les noms de domaine aux bureaux d'enregistrement. Et cela signifie que nous devons faire face à ces limitations dans le nombre de connexions. Parfois, on ne peut faire ces consultations que sur une heure, c'est le type de limitations qui sont imposées.

Les fondements pour ces limitations se rapportent évidemment avec quelque chose de raisonnable, à quelque chose de prudent pour l'exploitation du réseau. Ce serait vraiment bien si nous pouvions trouver une manière de permettre aux chercheurs reconnus ou accrédités pour qu'ils soient dans une liste sans ces obstacles, sans ces barrières. Mais nous nous battons pour obtenir cela pour le moment.

CATHRIN BAUER BULST : Merci beaucoup Dave. Je veux mettre l'accent sur la question de la responsabilité des acteurs individuels parce que je crois qu'il y a eu une réclamation spécifique sur un bureau d'enregistrement spécifique qui, en termes diplomatiques, faisait face à tout un bon nombre de cas d'usages malveillants. Et dans ce rapport, on disait qu'il était basé sur un rapport basé de janvier 2017. Voilà l'un des points mais ce n'est pas très récent. Donc s'il n'y pas cela, on aura une information sur une analyse continue de l'usage malveillant qui sera liée à des acteurs spécifiques et cela permettra donc d'avoir une transparence qui pourra, nous l'espérons, renforcer les efforts concernant la conformité contractuelle.

Il me semble que nous commençons à manquer de temps. Je ne sais pas si quelqu'un d'autre aurait d'autres questions avant la clôture de cette séance.

LAUREEN KAPIN : Moi, j'ai une dernière question. Je suppose que vous savez qu'il peut y avoir des changements dans le système du WHOIS. Ce que je voudrais savoir, c'est comment ces changements peuvent affecter l'initiative DAAR.

DAVID CONRAD : Le système DAAR en soi n'utilise pas une information d'identification personnelle. La seule identification et la seule information dont se sert DAAR au sein de l'ICANN qui est pertinente pour le rapport dont nous parlons est l'information du bureau d'enregistrement et le nom de domaine qui y est associé. Le reste de l'information est utile lorsqu'on essaie d'approfondir dans sa recherche, essayer de comprendre s'il y a un impact en particulier, un vecteur en particulier. Mais en fin de la rédaction de ce rapport, l'information du bureau d'enregistrement est la seule qui nous intéresse, dans la théorie. Au moins, cette information devrait être disponible sur le WHOIS public sans aucune limitation d'accès. Nous savons qu'il y a des débats qui se tiennent en ce moment concernant la décision finale sur l'information qui sera disponible pour le public et laquelle ne le serait pas. Mais nous en sommes encore à un débat en cours.

LAUREEN KAPIN : Merci beaucoup. Merci donc de tous les efforts concernant l'initiative parce que je sais que cette initiative sera bonne pour la communauté donc nous voulons vous remercier de tout ce travail.

Nous allons clôturer donc la première partie de ce débat du groupe de travail sur la sécurité publique. Nous avons mis l'accent sur l'une des initiatives de l'ICANN qui nous aidera à jeter un peu plus de lumière sur l'usage malveillant du DNS pour que la communauté soit au courant des tendances. Et cela peut nous aider dans l'élaboration de politiques.

[FIN DE LA TRANSCRIPTION]