LONDRES – Équipe de l'ICANN chargée de la sécurité, la stabilité et la résilience (SSR) - Session de sensibilisation
Mercredi 25 juin 2014 – 15h30 à 16h30
ICANN – Londres, Angleterre

JOHN CRANE: Bonjour à toutes et à tous. Je crois qu'il y a encore des gens au bar. Donc, j'espère qu'ils vont nous rejoindre. Donc, je suis responsable de RSS, ce qui veut dire sécurité, stabilité et résilience. Je suis à la tête de cette équipe. C'est un acronyme RSS. Vous savez à quel point nous aimons les acronymes. Donc, je vous parle un petit peu de ce que fait notre groupe, vous donner une mise à jour et vous présenter un petit peu certaines nouveautés technologiques, vous présenter notre équipe. En ce croirait encore dans les années 1990 avec ce gros appareil que j'ai entre les mains.

Donc, j'espère que vous pouvez lire ce qu'il y a à l'écran. Comme je dis, tout le monde n'est pas dans la salle, mais je m'appelle John Crane. Je suis à la tête de ce nouveau groupe. Ça revient du groupe sécurité qui existait auparavant. Dave Piscitello viendra nous dire quelques mots d'ici peu. Il est vice-président de la sécurité de la coordination ICT. Nous aurons également quelqu'un qui n'est pas avec nous aujourd'hui Carlos Alvarez qui est de Colombie et qui s'occupe du travail technique conformité et c'est quelqu'un qui beaucoup. Donc, au niveau technique et en Amérique Latine et dans la région des caraïbes où l'on parle très souvent espagnol. En tout cas, beaucoup mieux que moi.

Donc, il passe beaucoup de temps en Amérique Latine. Tomofumi Okubo n'est, hélas, pas avec nous aujourd'hui. C'est un spécialiste des systèmes analytiques d'idiotifiant. Il fait beaucoup de recherches également. Rick Lamb, responsable du programme du DNSSEC. J'espère qu'il va venir et nous avons Champika, déjà il y a tounga qui travaillait avec APENIC dans la région Asie pacifique. Il était à Brisbane en Australie et du bureau de Singapour de l'ICANN.

Il fait beaucoup d'engagement et de travail d'information à partir de Singapour et il est ne formation. C'est pour cela il ne peut pas donner formations. C'est pour cela qu'il n'est pas avec nous aujourd'hui et nous avons Steve Comte qui est responsable de la coordination de l'information. Et Deve est très occupé mais il va nous rejoindre.

Que faisons-nous? Pour la sécurité, groupe sécurité à l'ICANN, sécurité de l'internet. Donc, nous prenons en compte ces codes pour les sites web, la sécurité physique, la sécurité des réunions, la sécurité au niveau des identifiants. Donc, c'était vraiment quelque chose qui avait une grande envergure, très large et nous avons formé ce nouveau groupe l'année dernière et à la base, notre but est d'observer, d'évaluer et d'améliorer la sécurité et la résilience de l'internet dans les systèmes d'identifiants en collaboration avec les autres départements de l'ICANN. Essayer d'améliorer l'écosystème en général, d'améliorer la résilience.

Il y a quelques domaines fonctionnels qui sont un petit peu différents. Je vais entrer un petit peu plus dans les détails, un petit peu plus tard. Nous avons la préparation pour être prêt en cas de menace, en cas de risque pour faire face, pour la génération des domaines, ce type de problèmes, une collaboration basée sur la confiance. C'est travailler

avec la communauté, c'est un nom un petit peu complexe pour cela mais beaucoup de procédures analytiques. Donc, recherche sur la stabilité des identifiants.

Deve vient d'arriver, il peut enlever sa cravate et nous faire signe. Donc, nous allons commencer par parler de la prise de conscience des menaces qui existent dans les systèmes d'identifiant et puisqu'il vient d'arriver, Deve vient de courir pour arriver jusqu'ici, mais j'espère qu'il n'est pas trop essoufflé et qu'il peut prendre la parole.

DAVE PISCITELLO: Très bien, très bien. Oui, oui. Désolé d'être en retard, mais il y a trois réunions qui se passent en simultané ici comme d'habitude et c'est assez complexe à gérer comme calendrier. Donc, je m'appelle, John vice-président de la coordination sécurité, stabilité et résilience et je vais vous présenter un petit peu les quatre piliers des domaines fonctionnels qui existent pour cette équipe SSA et je vous présenterai d'autres membres de l'équipe Rick et Steve qui nous parlerons un petit peu plus de domaines sur lesquels ils se concentrent. Vous avez parlé déjà un petit peu de notre croissance, de la formation, de cette nouvelle équipe n'est-ce pas? Très bien.

Donc, sans plus attendre, la prise de conscience des menaces. C'est notre travail au quotidien. Nous sommes actifs 24/24, 7/7. Vous savez, on peut nous appeler à toute heure du jour ou de la nuit. On travaille avec des forces de l'ordre, on travaille avec des chercheurs en sécurité, avec des personnes qui interviennent au niveau des réseaux zombie et des activités malfaisantes sur l'internet, qui font des enquêtes.

Nous aidons les personnes lorsque l'on peut fournir des informations ou des renseignements. Nous le faisons. Nous sommes en contact avec plusieurs organisations. L'ICANN travaille peut être avec des bureaux d'enregistrement. Il y a des données qui doivent être synchronisées, des analyses qui devaient être menées et ce que nous essayons de faire c'est d'aider à contrôler le DNS pour qu'il n'y ait pas d'activité néfaste, d'activité criminelle.

Les forces de l'ordre peuvent venir nous demander pour mieux comprendre certains fonctionnements, l'identification d'informations lors de procès, d'affaire judiciaire devant les tribunaux. Parfois, on fait appel à nous pour les adresses internet protocole, pour les noms de domaine.

On passe beaucoup de temps à échanger des renseignements sur les différentes menaces qui existent. Nous participons à l'analyse de menaces, des attaques informatiques. Si nous avons des informations sur une attaque imminente sur le serveur racine ou sur un domaine de premier niveau, nous sommes en mesure de réagir très rapidement et de trouver des contre-mesures et d'effectuer des contre-mesures.

Voilà, j'ai besoin de changer mes transparents. Nous avons tout un groupe qui fonctionne de cette manière. C'est ce que nous sommes en train de développer, développer des informations des chiffres pour ce système d'identifiants parce qu'on a des demandes qui proviennent de la collectivité pour avoir une meilleure gestion plus uniforme du DNS.

On travaille beaucoup avec RSAC, avec la commission consultative. Nous espérons être en mesure d'avoir plus d'instruments pour chiffrer et

évaluer la situation. Moi, je me concentre principalement sur les abus d'enregistrement des sites web. On examine de manière très créative les données de domaines, les données pour les enregistrements. Pour le DNS, on essaye de comprendre quels sont les attitudes des criminels de l'internet.

Ils vont d'un d'enregistrement à un autre. Ils essayent de se cacher. On essaye de les poursuivre et de les suivre à trace et très souvent, on observe à partir de données, des tendances qui se dessinent et nous travaillons avec des personnes pour essayer de comprendre un petit peu ce qui se passe au niveau des données, extraction à partir des données, de tendances.

Donc, à partir de Los Angeles, nous tentons d'analyser de plus en plus la situation. Donc, c'est un travail à mi-temps pour trois personnes. Donc, on veut utiliser d'une manière créative les données DNS. Lorsque l'on pense à l'espace de sécurité, on sait que de collecter des données du DNS pour des parties tierces, ça, ça permet de mieux comprendre les comportements sur l'internet et c'est quelque chose d'important qu'on peut utiliser d'une manière très positive.

Donc, la collaboration basée sur la confiance, je crois qu'on participe tous à cette partie très intensive de notre fonction. Le cyber sécurité mondiale, coopération nécessaire pour ce cyber sécurité. C'est pour cela que nous communiquons avec beaucoup d'autres d'entités, avec d'autres acteurs de l'écosystème de l'internet, des groupes de travail, de l'ICT. Nous travaillons avec le Commonwealth, avec les Etats des caraïbes, avec Asie pacifique pour comment mieux partager notre savoir

et nos connaissances et acquérir ces connaissances que l'on peut par la suite partagée avec toute la communauté de l'ICANN.

Nous avons des opérations de sécurité globale qui se déroulent. On vous parlait de ces interactions quotidiennes au sujet des abus sur le DNS. Nous travaillons avec vraiment beaucoup de personnes sur des listes de publipostage. Une analyse complète, une recherche, en effet, des malicieux, des réseaux zombie, des programmes malveillants et nous prenons en compte les politiques de l'ICANN et nous assurons que si les politiques de l'ICANN ont quelque chose de néfaste pour la sécurité et la résilience de l'internet, on le fait savoir s'il vaut revoir certaines politiques qui pourraient être dangereuses pour la stabilité de l'internet.

On essaye de bâtir un petit peu plus de capacités. En fait, je vais demander à Steve de prendre la parole et il vient de revenir en notre sein et c'est Steve qui nous aide à coordonner nos programmes de formations. Je lui demandai d'en parler comment renforcer les capacités des personnes par la formation. D'où des formations sur le DNS. Donc, je vais prendre ce bel objet.

STEVE CONTE: Nous faisons beaucoup de formations et de renforcement des capacités depuis 2003 avec un centre de ressources, avec des formations ciblées sur les registres, les ccTLD et un transfert des connaissances très fort. Nous en faisons de plus en plus depuis 2007. Nous avons plus de partenaires et des formations sur le DNSSEC que fait Rick. Donc, des formations de déploiement DNSSEC. Donc, ça c'est vraiment

intéressant. Le DNSSEC a connu une forte croissance, vous savez, il y a de cela quelques années. Si vous avez suivi ces formations, je pense que vous avez entendu des experts régionaux qui sont tout à fait intéressant et Rick va nous parler peut être un petit peu plus de son travail dans le cadre du DNSSEC.

RICK LAMB: Donc, c'est de boutons qui font exploser quelque chose, non? Oui, comme l'a dit Steve, il ont lancé un travail. Moi je suis arrivé un petit plus tard. C'est vraiment des personnes qui nous ont été très utiles, qui ont été des fondateurs, des pionniers de cette équipe et ils m'ont beaucoup appris durant ces formations. On est en train de bâtir un réseau, de réseau de personnes, de formations de forces de l'ordre et d'autres personnes et je me rends compte que tout le monde dans la salle maintenant a dû suivre une classe sur le DNSSEC et il y a des personnes des forces de l'ordre qui m'ont parlé lors de ces cours, un samedi soir: quels sont les chances de contacter quelqu'un, quelqu'un qui me répond un samedi soir?

Ce qui compte c'est le réseautage, c'est de prendre des contacts. Ce n'est pas une approche hiérarchique que nous voulons obtenir ici. Non, c'est créer des réseaux, créer des contacts. Donc, on fait appel à nous pour des formations, pour créer par exemple un cadre de sécurité de cyber sécurité pour un pays. L'ICANN est un expert dans ce modèle multi parties prenantes. Nous savons, c'est quelque chose dont on a besoin dans tous les pays du monde.

Parfois, on fait appel à nos compétences à ce niveau, c'est quelque chose qui est gratuit et c'est quelque chose que l'on fait de par le monde et nous avons des technologies qui sont enseigner et nous créons des réseaux entre les différentes personnes qui assistent à ces cours qui durent une semaine. Voilà ce que je fais. Steve coordonne tout cela et je crois qu'il est très efficace. Il l'a rendu beaucoup plus efficace le processus.

SPEAKER: Combien de formations dans combien de pays?

RICK LAMB: Oui, je ne sais pas exactement. Ça ne fait pas très longtemps que je le fais, mais personnellement, j'étais dans au moins une quinzaine de pays.

STEVE CONTE: Merci Rick. Donc, nous avons un marché de plus en plus large. En 2012, on a parlé de sécurité publique beaucoup plus. Nous avons essayé de trouver les agences qui pouvaient bénéficier de nos cours, de nos formations sur la résilience, sur la sécurité et la stabilité de l'internet. et ces cours pour le personnel de l'ICANN parce que vous savez qu'il y a beaucoup de nouveaux personnels de l'ICANN qui vont être formés, qui connaissent mal ces concepts et nous les informons du fonctionnement du DNS et du DNSSEC et nous explorons une nouvelle piste de prise de conscience de la sécurité que nous voulons plus développer et je crois que vous allez voir beaucoup plus cela au début 2015.

Et nous allons promouvoir cela par l'intermédiaire de l'équipe d'engagement mondial. Vous en apprendrez plus à ce sujet. Donc, je ne veux passer trop de temps sur le public. On a commencé avec les opérateurs de registres ccTLD avec les bureaux d'enregistrement également qui sont venus nous voir pour en savoir plus sur la sécurité opérationnelle. On vous a parlé des dates comme 2007. On a développé véritablement ces programmes et on a été un petit peu en dehors de la communauté ccTLD. Donc, de plus en plus de cours, de formations pour avoir un impact beaucoup plus solide sur toute la communauté. On a déjà parlé de la sécurité publique au niveau de la communauté internet.

Donc, je crois que Champika est à Singapour en ce moment, en train de faire justement une formation à ce sujet. Donc, nous sommes toujours heureux lorsqu'on parle de SSR de nous déplacer et d'apporter notre expertise dans le monde entier. On peut fournir des formations à beaucoup de groupes sur beaucoup de thèmes. Donc, si cela vous intéresse, vous voulez une formation. Donc, combien sont des ccTLD dans la salle? Oui, quelques-uns. Oui, des bureaux d'enregistrement dans la salle. Levez la main, des gTLD qui sont dans la salle, des nouveaux, déjà existants. Très bien. Ça me donne une idée et catégorie autre. Très bien.

Vous savez, si cela vous intéresse, allez voir votre vice-président régional et nous serons très heureux d'essayer d'organiser une formation pour vous si vous avez une manifestation qui se tient avec beaucoup de personnes qui s'y rendent et que c'est en rapport avec le système d'identifiants, avec le groupe SSR de l'ICANN, avec le groupe sécurité, stabilité et résilience et nous sommes toujours très heureux.

N'hésitez pas à nous contacter directement si vous désirez une formation à votre réunion.

On essaye de travailler d'une manière plus stratégique et de par le passé, vous savez comment fonctionnait d'une manière un peu plus réactive c'est difficile. Plus on sait tôt quels seront les dates de cette manifestation, mieux cela sera pour nous. Tentons de travailler d'une manière stratégique. N'hésitez pas à nous parler très en avance parce que l'on peut préparer les choses très en amont et ça c'est toujours très utile.

Donc, vous avez beaucoup d'expérience dans la communauté. Il se peut que l'on rate quelque chose, qu'on ait oublié quelque chose. Vous savez, on fait ces cours depuis de nombreuses années. Ça marche, ça fonctionne, mais qu'est-ce qu'on pourrait fait d'autre. D'autres cours que l'on pourra proposer que l'on puisse concevoir. Donc, qu'est-ce qu'il manque. Quels sont les manques à combler au niveau de la formation, au niveau de ce que l'on peut apporter pour renforcer la sécurité de l'internet. Donc, si vous avez des idées, quelque chose qui pourrait être enseigné qui n'est pas encore enseigné, faites-le nous savoir. Vous avez sûr l'écran mon adresse email stevecomte@icann.org et sur ce je redonner la parole à John.

JOHN CRANE: donc, nous voulions vous donner un aperçu un petit peu de notre travail et maintenant, vous donner la possibilité de vous poser des questions. Peut-être qu'on ne sera pas en mesure de vous apporter une réponse,

mais n'hésitez pas à nous poser ces questions. Si vous pouvez utiliser le micro s'il vous plait dans la salle.

STEVE CONTE: Nous avons également des personnes en ligne

CASS GOLDING: Oui, je Nominet Uk TLD et ce que vous faites cette initiative mondiale est très apprécié, très utile. Je voudrai souligner est ce que vous avez des formations de formateurs où vous pouvez venir dans un pays et vous pénétrez dans une communauté pour former des formateurs?

STEVE CONTE: Nous faisons tout à fait des formations de formateurs, des formations ad hoc. Peut-être que vous pouvez nous en dire plus sur ce que vous avez fait. Mais, on essaye de travailler au niveau stratégique et on est que six dans l'équipe. Donc, c'est très important de faire la formation de formateurs pour diffuser les informations pour que les formations bénéficient d'un plus grand nombre de personnes et pour que plus de personnes soient prêts à fournir ces formations.

JOHN CRANE: On essaye aussi de trouver des mécanismes de formations en ligne pour qu'on n'ait pas à prendre des avions pendant des heures, mais, moi ce que j'aimerai dire, c'est que c'est bien d'être sur place, c'est bien d'être devant les étudiants. Il y a des choses qu'on ne peut pas faire en ligne.

La formation de formateurs c'est en effet ce qu'on veut faire, mais la formation sur place, le véritable transfert de connaissances de motivations est essentielle et être de visu devant les élèves, devant les personnes formées, les apprenants c'est quelque chose d'essentiel. Donc, je crois qu'on essaye évidemment puisqu'on est une petite équipe de faire à maximum maintenant de formations en ligne si possible.

STEVE CONTE: Vous avez deux membres du personnel qui vont prendre un rôle important dans cette formation. Carlos Alvarez va avoir un deuxième enfant. En fait, sa femme va accoucher aujourd'hui. Donc, oui, vous voyez. On était au courant, mais on est obligé de prévoir cela. Carlos Alvarez Travaille en espagnol et il va s'occuper de la région d'Amérique Latine. Il y a eu une formation en espagnol avec la documentation en espagnol. Moi, je vais aller le mois prochain à Singapour, Brisbane, dans toute la région Asie Pacifique pour former. Champika, Champi, on l'appelle. C'est plus court. Il parle chinois et il va pouvoir peut être travaillé à une formation en chinois et on a une demande de l'Interpol, de travailler avec l'Interpol et de faire une formation de formateurs pour le moyen orient et pour le personnel en français.

Donc, ça, ça serait une formation en français. On espère pouvoir les former en français avec Interpol. On a eu une réunion avec une dame d'une association qui s'appelle: Together against Cybercimre de l'université de Strasbourg. Ils sont très intéressés d'avoir des contenus en français, cette dame. Egalement, ça intéresse la langue russe. Donc, nous sommes de plus en plus multilingues. Nous aimerions travailler

dans toutes les langues des Nations Unies, les six langues des Nations Unies et donc le matériel, nous l'avons. Nous sommes très heureux de le partager et travailler avec vous pour délivrer ce matériel de quelque manière que ce soit.

CASS GOLDING: Merci beaucoup. Je prends note au micro dans la salle. En ce qui concerne les attaques dont vous avez parlé, les menaces qui existent sur les réseaux zombies. Est-ce que vous collectez des données au sujet de ces menaces DNSSEC. Donc, il y a beaucoup, beaucoup de données à collecter. Nous observons principalement.

C'est impossible de tout collecter. On cherche à avoir les mécanismes pour les menaces, pour justement, pour les opérateurs de serveurs. Il y a les serveurs racine qui avaient été éventuellement attaqués. Donc, nous serons en mesure de prévoir cela et d'avoir des mécanismes. Mais, vous savez toutes ces données qui existent sont nombreuses et ça fait peur. Quand on est des spécialistes de la sécurité, je ne suis pas sûr que toutes les unités d'attaque UDP vont être sur DNS, mais ça passe souvent au NTP maintenant. Donc, il faut savoir ce qui se passe faire du renseignement proactif pour voir d'où provenir les menaces

Et vous savez, il y a un an.

[FIN DE LA TRANSCRIPTION]