ICANN77 | Forum de politiques – Séance conjointe : ALAC et SSAC
Jeudi 15 juin 2023 – 13h45 à 15h00 DCA

YESIM SAGLAM: Bienvenue à toutes et à tous. C'est pour vous souhaiter la bienvenue à cette séance traditionnelle entre SSAC et l'ALAC. Nous allons devoir tout d'abord lancer l'enregistrement. La séance va commencer, nous allons lancer l'enregistrement.

Bonjour à toutes et à tous, bienvenue à cette séance conjointe ALAC/SSAC, je suis Yesim et je vais gérer la participation à distance pour cette séance.

Cette séance est enregistrée et suit les normes de comportement attendues de l'ICANN. Au cours de cette séance les questions et commentaires soumis dans le chat ne seront lus à voix haute que s'ils sont formulés dans la manière indiquée dans le chat. Je lirai les questions et commentaires à haute voix pendant la durée fixée par le président ou le modérateur de la séance.

L'interprétation pour la séance comprendra l'anglais, l'espagnol, le français. Cliquez sur le bouton d'interprétation dans Zoom et sélectionnez la langue que vous écouterez pendant la séance. Si vous souhaitez prendre la parole levez la main dans la salle Zoom et une fois que l'animateur de la séance aura appelé votre nom, activez votre micro. Avant de prendre la parole assurez-vous d'avoir sélectionné la

langue dans laquelle vous vous exprimerez si ce n'est pas l'anglais. Mettez en muet tous les autres appareils et notifications. Veuillez indiquer votre nom et parlez clairement et à un rythme raisonnable pour permettre une bonne interprétation de vos propos.

Cette séance comprend une transcription automatisée en temps réel qui n'est pas officielle et ne fait pas autorité. Pour la visualiser, cliquez sur le bouton close caption dans la barre d'outils de Zoom.

Pour assurer la transparence de la participation au modèle multipartite de l'ICANN nous vous demandons de vous connecter aux séances en utilisant votre nom complet, un prénom et un nom de famille. Vous risquez d'être exclus de la séance à défaut.

Je vais donner la parole à Joanna Kulesza, vice-présidente de l'ALAC.

JOANNA KULESZA: Merci, merci de vous joindre à cette séance traditionnelle entre ALAC et SSAC. Si vous regardez l'ordre du jour, je ne suis pas Jonathan Zuck, il va arriver dans la salle. Mais je vais parler très brièvement pour représenter nos invités et nous aurons également les liaisons SSAC qui vont nous rejoindre. Je sais qu'il y a des personnes qui sont à distance également. Donc nous allons avoir la présentation de ce à quoi on s'attend. Êtes-vous avec nous et en mesure de prendre la parole ?

ANDREY KOLESNIKOV: Oui, je suis ici et j'espère que vous m'entendez et que vous me voyez. J'ai allumé ma caméra.

Commençons cette réunion traditionnelle ALAC/SSAC, ça fait des années que cela se déroule, c'est une belle tradition. Passons directement à l'ordre du jour.

Nous allons structurer cette séance avec, tout d'abord Jonathan qui va dire quelques mots, puis Rod Rasmussen et nous allons parler des différents thèmes de l'ALAC et nous aurons des commentaires de clôture et les prochaines étapes. Mais nous commencerons par les thématiques concernant SSAC. La parole à Jonathan, à non, pardon à Rod Rasmussen, de SSAC.

ROD RASMUSSEN: Oui, c'est tout à fait intéressant, très content d'être avec vous aujourd'hui, avec l'ALAC. Nous allons parler de ces diverses initiatives qui nous intéressent. Il y a des nouveaux venus dans la salle, donc c'est important qu'avec ce comité consultatif, SSAC, nous parlions de nos avis que nous prodiguons au conseil d'administration concernant la sécurité et la stabilité de l'internet. C'est important pour les utilisateurs finaux également pour avoir un internet sûr et sécurisé.

Nous travaillons sur des thématiques communes qui sont nombreuses, sur l'alignement entre nos points de vue. Et c'est important de parler de ces différents avis sur ce qui nous concerne. Nous avons également des détails techniques qui seront abordés. Il y a des questions que vous pourrez avoir éventuellement, je pense que nous avons de nombreux experts à SSAC, de l'expertise, mais il y a également beaucoup d'experts à l'ALAC, je le sais.

Mais, néanmoins, voilà ce que je voulais vous dire. Donc nous allons parler maintenant avec différents membres de SSAC de divers efforts qui existent, il y a divers commissions et comités à SSAC.

On m'a rappelé de parler lentement et clairement, nous avons également parfois tendance, en tant qu'experts techniques à parler un peu trop vite.

Diapo suivante.

Nous allons donc avancer un peu et parler de la section collision de noms, donc on avance encore un peu, continuez, voilà, projet d'analyse collision de noms, c'est NCAP et nous avons quelqu'un qui n'a pas beaucoup de temps, Matt.

MATT THOMAS : Désolé de ne pas être ici en personne, j'ai eu des conflits personnels cette semaine. Je suis un des co-présidents du projet d'analyse sur les différentes collisions de nom avec Susan Wolf. Vous connaissez ces collisions de noms, cette problématique qui existe depuis des années, on en parle depuis de nombreuses réunions, mais je vais vous donner une petite mise à jour sur NCAP.

Nous sommes là pour répondre à des questions et donner des avis au conseil d'administration sur les collisions de nom. Il y a eu une demande de la part du conseil d'administration de l'ICANN pour. HOME,. CORP et. MAIL, on nous a demandé notre avis à SSAC pour d'éventuelles collisions.

On a travaillé avec la communauté ces dernières années, d'une manière inclusions. Il y a environ 25 membres du groupe de discussion et 14 membres des groupes de travail SSAC.

Prochaine diapositive.

Nous allons regarder ces récentes publications, nous avons la deuxième analyse NCAP avec 4 études, avec la question du conseil d'administration, comme cela a été indiqué. Mais il y a également 3 rapports séparés, des études de cas sur les chaines de collision, pour. MAIL,. MAIL,. HOME,. INTERNAL, .LAN et. LOCAL, en utilisant des données concernant les données du DNS à partir des serveurs racine A et J. Cela nous permet de voir les changements qui ont été effectués dans le cadre des requêtes du DNS et des altérations concernant le trafic.

Ce rapport a été conclu, il y a maintenant une période de commentaires publics et on va tomber à la suite de cette analyse sur un consensus.

Il y a également une étude sur la perspective des requêtes du DNS pour les domaines de premier niveau non existants. Cela nous permet de voir différents points de vue sur la hiérarchie du DNS, pour bien comprendre quelles sont les limites existantes lorsque l'on parle de collision de noms, lorsqu'on utilise les données qui peuvent être utilisées pour évaluer les collisions de noms à l'avenir.

Là aussi il va y avoir un commentaire public et on a un appel à consensus dans le cadre de ce débat.

Ce que l'on n'a pas sur cette page est un troisième rapport qui a été conduit par le groupe d'études techniques pour l'étude 2 de NCAP afin

d'analyser les rapports de collision de noms reçus par l'ICANN depuis 2012 jusqu'à maintenant pour faire une analyse des causes sous-jacentes des collisions de noms. Ce rapport est en train d'être finalisé et il n'y aura pas de commentaires publics, mais ce sera le 5ième rapport qu'on nous avait demandé, un rapport solide et fortement étayé pour le conseil d'administration, répondant à ses questions avec beaucoup d'informations qui sont pertinentes pour le conseil, pour voir comment on peut régler la question des collisions de noms à l'avenir.

Diapo suivante.

Quels sont les résultats clefs et principaux que nous avons obtenus à NCAP ?

Nous avons un problème avec ces collisions de noms au niveau du DNS. Et, véritablement, cela provient de protocole de découvertes de service et des listes de recherche de suffixes qui posent problème dans le DNS. Il y a également ces indicateurs de diagnostics critiques qui sont définis pour mesurer les collisions de nom. On parlera de ces CDM d'ici peu.

Mais ce qu'il faut bien comprendre, ici, c'est que plus on a de CDM en volume et en diversité, ça veut dire qu'il y a diverses dimensions qui sont analysées, le nombre de réseaux, de noms de domaine. Et la limitation et la remédiation sont problématiques. Il y a un volume de plus en plus difficile à gérer, une diversité de plus en plus grande de mesures de diagnostics critiques. Il est très important d'avoir une plateforme de mesures et d'indicateurs pour voir quelles sont les priorités pour voir quand il va y avoir des dossiers de demande déposés, pour prendre des décisions informées sur d'éventuelles collisions de noms entre chaines.

Diapo suivante.

Les éléments critiques de mesure dont je vous parlais ces CDM, et bien c'est ce qu'on utilisait en 2012 également. Donc ces mesures analysaient le volume de requêtes, la diversité de l'origine des requêtes, la distribution des adresses IP, la distribution des numéros de systèmes autonomes ASN, la diversité au niveau de type, diversité des étiquettes également. Et ça, c'est un travail d'investigation que nous avons réalisé pour véritablement découvrir d'où proviennent ces collisions au niveau du DNS public et voir également les problèmes que cela peut poser.

Diapo suivante.

Le groupe, donc, à la suite de l'étude 2 veut s'assurer que les collisions de noms puissent être évaluées. Pour que cela soit possible, il faut que les collisions soient visibles si elles existent. Il a été noté qu'il y avait un fossé technique entre 2012 et maintenant. Parce que l'écosystème a beaucoup changé au niveau de DNS depuis 2012 et il a des résolveurs publics par exemple, il y a des ensembles différents, il y a des noms de domaine qui n'existent plus. On se basait autrefois sur d'autres observations, d'autres capacités sur la zone racine qui étaient évaluées.

Donc, pour se faire, nous avons proposé un flux de travail différent, toujours dans l'esprit de 2012, mais nous voulons nous assurer d'analyser les collisions de nom d'une manière durable et pertinente pour faire plus de remédiation, notamment.

Voilà un peu ce à quoi ressemble ce flux de travail et ce calendrier. Ce qu'il y a d'important et qu'on voit ici, c'est que vous avez des options de lancement. On a beaucoup réfléchi à cela. Il faut que les dossiers de

demandes ne soient pas coincés comme on l'a vu avec. HOME,. MAIL et tout ça.

Donc nous avons 4 opportunités pour que les dossiers de candidature soient retirés ou annulés. On commence avec une évaluation statique de la chaine qui est demandée dans le dossier de candidature. Il y a des opportunités pour des plateformes. Il y a des plateformes qui existent déjà, comme le système ITHI, il y a des données déjà disponibles pour les candidats avant de soumettre une chaine. Il faut qu'ils aient la possibilité de faire des tests pour voir si la chaine qu'ils vont demander ne va poser problème de collision.

Ensuite, on a le début du processus de dossier de demande, nous avons l'équipe technique de révision qui fait une évaluation de statuts. Je reviendrais là-dessus un peu plus tard. Là, on analyse les données qui sont disponibles publiquement. Il y a une évaluation qui est réalisée au niveau de l'impact de la chaine sur les collisions de noms. Et là, il y a la possibilité de sortir une nouvelle fois. Si la chaine pose problème, le dossier peut être retiré à ce niveau, au niveau des serveurs de différents noms. Et cela est possible au niveau de l'évaluation de collision passive, PCA. Là aussi, il y a une possibilité de sortir à ce niveau-là s'il y a un problème au niveau des données, si cette chaine ne peut pas fonctionner, s'il y a une collecte de paramètres à ce niveau qui vont prouver cela.

Donc, là on gère certains problèmes techniques, comme je l'ai décrit plus tôt au niveau du DNS, au niveau des informations qui existent déjà, au niveau des risques qui existent de collision de noms

Une fois que l'on passe à la période suivante, s'il n'y a pas de risque identifié par l'équipe de révision technique, on poursuit. Sinon il y a la possibilité de sortir.

Ensuite nous avons la période ACA, évaluation de collision active. Et là, s'il n'y a pas de réponse pour une chaine, ça permet de vérifier la capacité des adresses protocole internet IP, tout cela est contrôlé par l'équipe technique et on voit quels sont les logiciels qui pourraient déjà utiliser cette chaine. Donc on informe la possibilité de collision de noms de domaine à ce niveau. Et à ce moment, on peut sortir un dossier de candidature s'il y a des risques pour la stabilité du DNS, il y a différentes recommandations à ce niveau qui sont envoyées au conseil. Toutes les évaluations sont envoyées au conseil d'administration qui va décider et statuer de l'évaluation du risque de collision par rapport aux noms.

Il y a deux fonctionnalités importantes de ce flux. Donc l'équipe TRT, ce sont des gens qui doivent bien comprendre le DNS et le fonctionnement de l'infrastructure de l'internet et quelle est l'interface du DNS sur les applications et les services. Ils doivent comprendre les fonctions de la gestion de diagnostic critique et comment réussir dans l'exploitation de ce modèle.

Il y a 4 responsabilités : l'évaluation, la documentation, les recommandations, évaluer les plans de remédiation et d'atténuation et aussi avoir une fonction de réponse de secours.

Ensuite, il y a aussi un prestataire de service neutre, c'est une entité qui peut être séparée de l'équipe TRT. Et donc ce sont des responsabilités

qui sont l'opération de l'évaluation de collision passive et active, l'analyse et être une équipe a fonction de réponse/réaction de secours.

Je noterais que le groupe est en cours de finaliser ses analyses et recommandations, nous serons heureux d'avoir de nouvelles personnes qui pourraient se joindre à nous. Si vous êtes intéressés, les informations sont à l'écran, ou vous pouvez me contacter. Je répondrais volontiers à vos questions.

ROD RASMUSSEN: Y a-t-il des questions dans la salle ou sur Zoom ? Il n'y a pas de question. Jonathan ?

JONATHAN ZUCK : Je pose une question de non-expert. Je suis fasciné par ce concept d'évaluation du risque. Il y a différents niveaux de responsabilité pour les candidats en fonction du risque pré-évalué ou alors est-ce qu'on décide de déposer sa candidature et après l'ensemble de responsabilités est le même ? Est-ce qu'il y a un seuil dans le travail quantitatif qui dit que vous devez atteindre tel niveau de rigueur si vous avez tel niveau de risque ?

MATT THOMAS : Très bonne question. Avec ces mesures quantitatives, il n'y a pas de chiffre magique où on dirait qu'au-delà de ce niveau de volume de requête ce serait cela ou ceci. Donc c'est un critère subjectif, qualitatif, quantitatif qui nécessiterait l'expertise de l'équipe TRT.

ROD RASMUSSEN: Y a-t-il d'autres questions ? Matt l'a dit, nous arrivons à la fin de cette partie, nous aimerions obtenir des commentaires mais c'est déjà assez tard. Ce sont les mêmes diapos que nous avions la dernière fois.

Le NCAP est très important, donc je voudrais que vous le sachiez, nous avons une très bonne réunion ici à Washington et nous essayerons d'avoir d'autres réunions en présentiel pour poursuivre notre élan.

Nous sommes prêts pour que les autres fassent les lancements qu'ils jugent nécessaires.

Pouvons-nous revenir en arrière dans le diaporama où on parlera de l'automatisation de la délégation de signature ? Peter va nous parler de ce sujet. C'est le même sujet, ce sont les mêmes diapositives que nous montrons, mais nous avons fait des progrès depuis.

PETER THOMASON: Ces diapositives semblent ne pas être complètement à jour, il nous faut procéder avec ces diapositives.

Nous l'avons déjà dit dans le cadre de ce forum, quand vous avez un domaine, le DNSSEC a une rotation de clefs, quand les clefs changent il faut absolument mettre à jour l'enregistrement relatif à la signature. Donc quand le bureau d'enregistrement est aussi le fournisseur de ces clefs. Cela n'est pas toujours le cas, il faut alors fournir les informations nécessaires à l'opérateur de registre. Le processus peut être compliqué. On nous dit que 40 % des titulaires de domaine réussissent à prendre les

mesures nécessaires. Ce qui est nécessaire c'est davantage d'automatisation. Il y a plusieurs façons de procéder.

À la diapositive suivante, je vais en parler davantage.

Nous avons un diagramme qui montre la procédure manuelle. Tout en bas vous avez le niveau enfant et en haut le niveau parent et au milieu vous avez le titulaire de domaine et le revendeur. L'opérateur a donné son autorité et quand ce n'est pas le même que le bureau d'enregistrement, alors le bureau d'enregistrement obtient les données du revendeur. Les données remontent jusqu'au TLD. La difficulté ici, dans cette étape intermédiaire, vous la voyez.

Diapo suivante.

Il y a déjà une certaine automatisation, pour les ccTLD il y en a 10 qui ont cette automatisation. C'est quelque chose qui est indiqué, le niveau parent peut découvrir la situation en recherchant les données, c'est le scanning CDS.

Cela pose plusieurs problèmes, il y a un temps de conversion quand la conversion est réalisée, le titulaire de nom de domaine ou l'opérateur DNS ne sait pas à quel moment le changement va se faire, cela peut prendre toute une journée.

Ensuite il y a un problème d'échelle. Bien sûr, plus la fréquence est importante, par exemple si c'est toutes les heures, ça peut être une charge 24 fois supérieures. Tout dépend du nombre de domaines qui ont une délégation sécurisée. Il faut que le scan se fasse tous les jours.

Il ne semble pas qu'il y ait un problème pratique en fonction du nombre d'opérateurs de registres ccTLD, mais il pourrait y avoir des complications à l'avenir, surtout si les choses deviennent plus strictes.

L'une des atténuations qui pourraient être introduites pour éviter les problèmes serait d'améliorer les scans opportunistes qui se déroulent tous les jours et il faudrait un déclencheur. Donc l'opérateur DNS dirait, le parent, voilà j'ai mis un dispositif dans le niveau enfant. Cela s'appelle Notify et vous en avez peut-être entendu parler, la généralisation n'a pas encore été spécifiée et il faudrait que cela soit fait et les logiciels adéquats devraient être élaborés. C'est encore loin devant nous.

En plus du modèle RRR, il y a deux acteurs. L'opérateur de registre et le bureau d'enregistrement. Les deux pourraient regarder les enregistrements et l'opérateur de registre pourrait rechercher directement les données au risque que le bureau d'enregistrement ne connaisse pas les données nécessaires et il y aurait un problème de synchronisation. Qui pour regarder le scan ? Il semblerait que ce soit peut-être le bureau d'enregistrement. Ce serait l'approche la plus fluide, et il y a un bureau d'enregistrent, en Norvège et il y a aussi 10 opérateurs de registre ccTLD qui le font.

Par exemple si l'un de ces opérateurs de registre le fait, il y aurait donc deux acteurs qui scanneraient et il y aurait peut-être une collision et il faudrait peut-être un accord entre l'opérateur et le bureau d'enregistrement. Cela semble compliqué, donc l'approche scan peut sembler facile, mais il y a toujours des détails.

Ici c'est un diagramme qui nous montre la simplification de la couche de scan, vous voyez la couche intermédiaire, entre le parent et l'enfant, où on ne fait plus de choses manuellement, on peut faire le scan directement. On a les données directement du serveur faisant autorité. Et on met à jour les données DS et on fait savoir au bureau d'enregistrement ce qui doit être fait.

Et il est possible que la base de données du bureau d'enregistrement soit dans le noir.

Ensuite, il y a une approche plus naturelle. Le bureau d'enregistrement est la partie qui reçoit les informations DS manuellement du titulaire du nom de registre, le scan c'est la flèche 2, ce serait simplement une autre façon pour le bureau d'obtenir les mêmes informations de la part de l'opérateur DNS et ainsi le bureau d'enregistrement fait suivre ces informations à l'opérateur de registre.

Diapo suivante.

Nous avons des positions préliminaires à SSAC. Ici ce sont des informations préliminaires. Nous établirons les détails au cours des semaines à venir et nous espérons avoir un port avant la prochaine réunion d'ICANN en octobre à Hambourg.

Les positions préliminaires sont les suivantes. Le DNSSEC est très difficile à établir pour beaucoup de personnes et l'adoption DNSSEC est très faible. Donc en ce qui concerne l'automatisation DS, elle pourrait être accélérée. Pour cela il faudrait travailler avec l'équipe de mise en œuvre de l'automatisation pour soutenir la participation au processus

ITF pour résoudre les problèmes de retard dans tout le processus de scan.

Nous avons aussi des domaines qui ne sont pas dans la catégorie ccTLD ou gTLD mais dans la catégorie RRR et Ripe s'en occupe. Donc des conseils similaires devraient être fournis à ces parties.

Nous avons aussi un arrangement qui est idéal, d'avoir des mises à jour DS qui seraient communiquées aux bureaux d'enregistrement. Les bureaux d'enregistrement devraient inclure le soutien à l'automatisation dans leurs prestations de services et ainsi ils auraient le contrôle des procédures.

Voilà ce que j'avais à dire sur cette mise à jour. La partie Notify implique aussi un envoi de la part des opérateurs DNS. C'est un groupe d'entité qui serait impliqué par cet avis. Dans l'idéal les opérateurs de DNS enverraient les messages correspondants chaque fois que les enregistrements relatifs à la signature de délégation doivent être mis à jour. Mais c'est encore très tôt pour faire cette recommandation. C'est encore une étape très préliminaire.

C'est la fin de mes diapositives, je peux répondre aux questions.

ROD RASMUSSEN: Y a-t-il des questions en ligne ou dans la salle ? Jim ?

JIM GALVIN: Je voudrais dire que je ne sais pas si l'ALAC a une position ferme sur les questions relatives au DNSSEC, mais l'ALAC considère que les

enregistrements relatifs à la signature de délégation ont un impact sur les utilisateurs. Ces choses peuvent paraitre très techniques et on ne se rend pas compte immédiatement de ce qui se passe exactement.

Nous encourageons l'ALAC à réfléchir à cela, nous avons des personnes telles que Peter et d'autres dans le groupe de travail qui seraient heureuses de vous éclairer. Mais dites-nous ce que vous pensez pour envisager si vous souhaiteriez avoir un rôle dans l'avancement des choses. En tout cas, je ne voudrais pas m'exprimer au nom de SSAC.

ROD RASMUSSEN: Vous pouvez vous exprimer au board. Je voudrais ajouter à ce que Jim disait. Nous avons eu un atelier DNSSEC, nous en avons un à toutes les réunions de l'ICANN, donc ici ça a été une demi-journée au forum politique. Donc il faut mettre cette thématique dans un contexte. Pourquoi passons-nous tellement de temps à parler de cette thématique un peu ésotérique ?

C'est un peu une fondation pour DNSSEC. En jeu, c'est l'adaptation de DNSSEC et cela a un impact sur les personnes qui voudraient créer de nouveaux services et qui pourraient bénéficier d'une cryptographie faisant l'objet d'une confiance universelle. Et cela serait utile pour qu'il y ait une harmonisation dans ces iles de confiance. Et cela pourrait être utile du point de vue opérationnel et gouvernemental.

On se demande pourquoi nous passons autant de temps, déployons autant d'énergie pour finaliser toutes choses, ces éléments. C'est très important afin que les entreprises puissent être dans la confiance, savoir qu'ils peuvent exploiter leurs entreprises en toute sécurité.

Nous enregistrons les séances et n'hésitez pas à parler à tous les membres de SSAC, surtout à Jacques qui a fait des choses très intéressantes au Canada et il a réussi à faire en sorte que les différentes provinces puissent interagir les unes avec les autres. Et il faut un acteur comme DNSSEC pour faire fonctionner tout cela. Car, au bout du compte, le bénéfice est pour les utilisateurs de l'internet.

JONATHAN ZUCK : J'ai un petit peu oublié ma question, mais je crois que la communauté At-Large, aussi avant moi, a pris la collision des noms avec beaucoup de sérieux et c'est très important pour nous. On n'a pas encore véritablement pris une position sur le DNSSEC, nous soutenons le DNSSEC et son utilisation. Nous l'avons vu dans des commentaires publics, mais si on peut faire quelque chose de plus créatif pour promouvoir l'utilisation du DNSSEC, comment on peut utiliser ces systèmes qui sont vraiment apportés par l'ICANN et importants pour les utilisateurs finaux, nous le ferons.

Il faut voir quels sont les mécanismes très utiles pour les utilisateurs et on peut faire passer le message.

ROD RASMUSSEN: Oui, c'est aligné avec ce que nous allons faire en septembre dans un atelier, au niveau du DNSSEC et de la sécurité. Puisque là on parle d'extension de sécurité.

Nous allons également travailler avec le département des communications de l'ICANN pour créer des messages et promouvoir

cela. Donc ce serait bien de collaborer au niveau de cette promotion, parce que vous êtes un canal de communication de ces thématiques.

Une question de Hadia ? Nous avons un écho, ça n'a pas fonctionné, on va réessayer.

HADIA ELMINIAWI: Je crois qu'At-Large pourrait promouvoir l'adoption du DNSSEC, mais nous ne sommes pas tous des spécialistes de la technologie. At-Large se sont des personnes qui ne sont pas spécialistes de la technologie, comment promouvoir l'adoption du DNSSEC sans être expert ?

ROD RASMUSSEN: Oui, c'est une bonne question, on doit réfléchir à cela et y travailler. Je crois qu'en fin de compte, ce n'est pas la technologie en elle-même c'est ce que l'on peut faire avec cette technologie. Donc avec des études de cas.

Et je parlais du travail de Jacques au Canada. Tout le monde, par exemple au Canada, si on a tout en virtuel comment prouver son âge avec une carte d'identité ? Mais on peut passer par d'autres systèmes. Il y a des canadiens qui vont dans des bars à Tokyo, ce sont des exemples donnés.

Et les utilisateurs finaux qui veulent faire quelque chose, il faut que la technologie leur permette de faire cela. Et je crois qu'on peut parler de ces technologies et les promouvoir, se faire l'avocat de ces technologies.

Mais pour que cela fonctionne bien, on a besoin de ces technologies.

MATT THOMASON: J'aimerais rebondir là-dessus. On veut s'assurer qu'il y ait moins de piratage avec le DNSSEC, que cela fonctionne mieux, que cela protège mieux les noms de domaine. Parce qu'il y a un système d'encryption qui a été utilisé ces 10 dernières années et cela est très intéressant pour le trafic, notamment sur la zone P.

Je crois que le DNSEEC, si vous avez un nom de domaine, vous devez être en mesure de le sécuriser avec les dernières technologies disponibles, comme on utilise le TLS pour le site web, comme on a une voiture avec des airbags et des protections.

ROD RASMUSSEN: Barry ?

BARRY LEIBA: Oui, Rod et Peter ont répondu, c'est pourquoi on devrait promouvoir cela et qu'est-ce que vous pouvez faire pour promouvoir cela en tant que personnes non techniques. Et je crois que la réponse c'est que la communauté At-Large pourrait travailler avec les opérateurs, avec les prestataires de service et avec les utilisateurs et poser la question : utilisez-vous le DNSSEC ? Pourquoi et comment cela fonctionne ? Si on paye pour des services de prestataires et bien il faut leur demander s'ils sont au niveau technologique et s'ils utilisent le DNSSEC.

AMRITA CHOUDHURY : Ce que l'on peut faire c'est d'être un canal d'amplification, mais on a besoin de communication précisément faites pour différentes cibles. Par exemple quand on parle à des personnes responsables de politiques, on doit expliquer pourquoi c'est important, pour un prestataire de service internet là c'est un autre message à passer avec un autre type de communication et de langage.

Donc lorsque vous avez ces communications, il faut voir ce dont on a besoin pour que la communication soit efficace. Et voir comment également ça peut être promu dans différentes régions ou pays. Parce qu'il faut voir si les utilisateurs finaux peuvent soutenir cela. Ça dépend donc des différentes régions, ça dépend des techniques de communication qu'on va utiliser.

ROD RASMUSSEN: Merci beaucoup, c'est noté. Je crois que je vais continuer à travailler avec l'équipe de communication de l'ICANN. Je vais avancer un peu dans nos présentations à moins que vous ayez une question. Hadia ?

HADIA ELMINIAWI: Oui, très rapidement. Moi je dirais que tous les opérateurs de registre sont au courant du DNSSEC et ceux qui ne le mettent pas en œuvre ont diverses raisons pour cela. Donc pour être en mesure de promouvoir cela nous avons besoin de travailler ensemble sur l'obtention de réponses et de raisons pour lesquelles le DNSSEC n'est pas mis en œuvre. Et on doit travailler ensemble à créer un nouvel espace, en effet, dont vous parliez.

ROD RASMUSSEN: Oui, où se situe le problème, est-ce que cela vaut la peine de travailler à ce problème, est-ce qu'on peut obtenir des résultats. Donc c'est une conversation intéressante sur le DNSSEC et ses extensions de sécurité. Ça va nous permettre de préparer nos conversations à ce sujet.

On me fait un signal, je crois que nous avons une question en ligne. C'est un commentaire de John, très bon commentaire concernant les revendeurs. Oui, les ISP et les bureaux d'enregistrement peuvent être éduqués sur le DNSSEC, ce qui est difficile c'est que les revendeurs et développeurs adoptent le DNSSEC, cela représente 25 % du marché des gTLD. Excellente observation de John en ligne.

Nous allons passer au point suivant, on doit avancer.

Donc le programme des nouveaux gTLD, la mise en œuvre de la nouvelle série. On avait parlé un peu de NCAP concernant la nouvelle série de gTLD et il y a de nouveaux développements à ce niveau. Avec le document SSAC 114, nous voulons parler de cela.

Nous allons avoir des amendements aux contrats, vous le savez, et je suis sûr qu'il y aura des commentaires concernant ces amendements. Ça c'est au niveau des réponses à apporter.

Il y a des études également qui sont effectuées par l'institut de l'utilisation malveillante du DNS et par l'ICANN. L'ICANN ne fait pas les études mais finance ces études. C'est une grande distinction. Et je crois que c'est bien qu'il y ait des études indépendantes, ce sera moins perçu comme étant politique. Mais ça ne va pas nous donner l'opportunité de

commenter sur l'avancée de l'étude. Je crois que ça va être l'université de Genoa qui va faire cela.

Donc j'ai parlé avec le directeur de la technologie à ce sujet. Il y a différents conseils qui vont être donnés aux chercheurs. Donc on va faire cela en tant que SSAC, donner des paramètres, voir quoi rechercher, quelles données rechercher, essayer de bien comprendre les causes et la prévalence de l'utilisation malveillante du DNS au niveau de certains bureaux d'enregistrement et registres et je crois qu'ALAC sera très intéressé par cela également. Nous partagerons tout cela avec vous. C'est une excellente opportunité.

C'est une question de processus, quand sera-t-il lancé ? On aimerait voir l'étude faite rapidement pour que ça ait un impact sur le processus et sur l'évaluation de l'utilisation malveillante du DNS et l'impact que cela aura sur la nouvelle série de gTLD. Donc peut-être que Jonathan veut rebondir ?

JONATHAN ZUCK : Non, c'est bon. Nous sommes en ligne là-dessus. On va voir, je crois, des débats là-dessus, et ces amendements contractuels sont importants. Donc s'il y a besoin d'un PDP pour gérer certaines des découvertes effectuées par ces analyses, ça pourrait être important. Nous avons eu des bruits externes.

ROD RASMUSSEN: Nous avons des interférences sur la ligne, quelqu'un a un micro ouvert.

Nous allons parler avec Gautam, qui est maintenant membre de SSAC, ça a été approuvé par le conseil d'administration, mais officiellement c'est un invité qui est en processus d'approbation et qui va nous rejoindre prochainement en tant que membre. Gautam ?

GAUTAM AKIWATE: Oui. Nous allons parler de la gestion du registre NS et de différents produits concernant les pratiques des bureaux d'enregistrement qui ne sont pas documentés.

Il y a des limites au niveau de l'EPP, du protocole d'avitaillement extensible et des politiques concernant les registres pour le retrait de domaines expirés. Donc les bureaux d'enregistrement ont exposé certains domaines à diverses résolutions en cas de piratages de domaine.

À la diapo suivante, nous avons cette information sur le document dont je suis l'auteur et qui prend en compte beaucoup de domaines sensibles. Il y a différents domaines dont vous pouvez avoir la liste. On peut avoir ce document qui s'appelle Risky Business, les risques dérivés par la gestion des noms concernant les bureaux d'enregistrement. Ça c'est les aspects techniques.

Mais les bureaux d'enregistrement et les registres nous ont demandé ce que l'on peut faire au niveau technique de SSAC. Donc on se concentre sur deux choses : comment limiter les risques actuels de piratage pour certains domaines qui ont été piratés. Un tiers de ces domaines ont été piratés par de mauvais acteurs qui utilisaient d'une manière malveillante ces domaines.

La deuxième question que nous avons c'est : quelles sont les options qui existent pour, une nouvelle fois, limiter les problèmes, pour que cela ne se reproduise pas à l'avenir. Ce qu'on essaye de voir c'est les différentes options qui existent dans notre cadre, quel est le niveau technique nécessaire pour toutes les parties prenantes. Et, dans tous ces cas, est-ce que c'est titulaires de noms de domaine qui peuvent faire quelque chose, les bureaux d'enregistrement qui peuvent réagir ?

Nous sommes en train d'analyser cela. Les titulaires de nom de domaine doivent être responsables aussi de vérifier que leur domaine fonctionne bien, est à jour et à niveau. Et qu'il n'y a pas eu de piratage par exemple.

Il faut voir également quelles sont les responsabilités qui existent pour les bureaux d'enregistrement, pour les registres et les parties prenantes également doivent voir s'il existe de nouvelles pratiques qui mettent les domaines à risque de piratage.

ROD RASMUSSEN: Merci. Donc nous avons inclus cela, la coopération avec les différentes parties prenantes qui ne sont pas obligatoirement membres de SSAC mais avec qui nous allons collaborer. Nous avons besoin de partager de l'expertise.

Donc je pense que cela fonctionnera bien. Nous allons une nouvelle fois lancer un message aux bureaux d'enregistrement et aux registres pour travailler sur ce problème de gestion de ces noms de domaine.

Y a-t-il des questions sur ce sujet ?

Donc nous allons faire des progrès sur ces points et nous vous tiendrons au courant d'ici Hambourg, nous aurons avancé et nous pourrons faire des recommandations éventuelles et les présenter à Hambourg.

Diapo suivante s'il vous plait. Les politiques de transfert, rien n'a changé depuis qu'on s'est vu. Il ne faut pas oublier le DNSSEC quand on transfère le nom de domaine, c'est aussi simple que cela. C'est vraiment important et dans la portée de notre travail.

Dernier point, un sujet que l'ALAC nous a demandé de traiter, c'est l'alignement sur .ZIP. Certains membres étaient préoccupés par cela. Et certains des membres de l'ALAC également.

JONATHAN ZUCK : Oui, ça, ça a été délégué il y a de nombreuses années. Donc ZIP et MOVE ont été délégués en 2012 et je crois qu'il y a beaucoup d'idées à cela, ce sont des noms de domaine génériques. Et il y a eu des chercheurs sur la sécurité qui ont vu s'il y avait des problèmes associés avec ZIP et MOVE parce que ce sont des extensions qui sont supposées être de confiance. Donc des vidéos ont été effectuées pour montrer comment créer de fausses URL qui ressemblent à des pièces jointes et il y a des utilisations malveillantes à ce niveau avec ZIP.

Et il y a trois éléments à ce sujet. Le premier : qu'est-ce qui peut être fait maintenant, si c'est possible ? De l'information et de l'éducation des utilisateurs ? Je n'ai pas la réponse à cela.

J'ai une réponse productive avec Crystal Ono de Google qui nous a dit suivre de près la situation pour voir s'il y a beaucoup d'abus qui existent

avec .ZIP et .MOVE. Donc on a fait des essais avec des pièces jointes, des tests ont été réalisés. Donc on essaye de voir ce qu'on peut faire. Mais ils n'ont pas encore noté trop d'abus à Google. Mais ça ne fait pas très longtemps que l'enquête a été lancée. Mais ils sont bien situés pour suivre de près la situation.

Donc nous avons cette assurance de leur part, ils nous ont rassurés.

Il a un blog également de Google où il y a beaucoup de fichiers, de formats qui ressemblent à des noms de domaine, qui utilisent des noms de domaine, mais il y en a peu qui sont tombés dans cette catégorie de reconnaissance générale où on est sûr qu'on peut utiliser ces extensions.

Là vous avez parlé des collisions de noms, moi je crois que les URL peuvent poser problème. C'est un petit peu comme des collisions d'URL, pas seulement de noms. Et je crois que l'évaluation des risques pour les utilisateurs est importante, c'est pour cela que nous voulions en parler avec vous.

Et la dernière question, c'est est-ce qu'on devrait essayer, avant la nouvelle série, de voir les différentes extensions comme JPJ et autres, où les gens cliquent automatiquement et ils sont en confiance quand ils voient ces extensions. Je pense qu'il faudrait réfléchir à cela avec vous.

Voilà pourquoi on vous a posé la question, parce que vous êtes des spécialistes de technologie et vous avez des projets à ce niveau.

ROD RASMUSSEN: Oui, ce sont des questions intéressantes. Et, d'une certaine manière vous avez ce problème lorsque quelqu'un s'enregistre avec un nom inconnu et fait du hameçonnage. Nous envisageons la collision des noms comme étant quelque chose qui fuite dans le DNS, c'est de notre point de vue, c'est ce que nous regardons dans nos études sur la collision des noms. Mais ça, c'est très similaire en ce sens qu'il y a des interactions intéressantes qui peuvent se produire.

Mon prestataire de télévision vient de m'indiquer qu'il fallait que je l'appelle, il veut me vendre des services, désolé.

Nous avons mené des discussions sur quel est le contexte, que se passe-t-il, quelles sont nos problématiques. Nous en avons décelé plusieurs. Un, c'est le système d'exploitation et ceux qui l'on créé. Plusieurs personnes l'ont créé, il y a des façons de démêler tout cela si vous considérez qu'une extension pourrait faire quelque chose.

Il y a aussi le problème de l'interface humaine, ça c'est plus compliqué parce que vous avez regroupé tout un tas de fonctionnalités en une seule. Votre navigateur doit être en mesure d'interpréter ce qu'il doit faire avec certains éléments. Donc si vous faites des suppositions paresseuses sur ce qu'est un TLD donné cela peut être assez intéressant.

En ce qui concerne .ZIP, l'eau a coulé sous les ponts, cela a été délégué, personne n'est aux abois en train de crier que les ponts sont en train de s'écrouler, il n'y a pas vraiment de choses pratiques à entreprendre.

JONATHAN ZUCK : Oui, en fait, il y a des gens qui sont aux abois parce qu'il y a des gens qui voient des problèmes quand ils sont chez eux.

ROD RASMUSSEN: Mais je ne vois personne qui soit représentant d'une autorité gouvernementale ou autre qui se soit signalé.

Donc, en réalité, peut-être qu'il y aura un problème pour ICANN Org à répondre à ces questions.

Voilà l'étendue de mes connaissances. Nous avons des experts cependant. Je vous ai dit que j'allais encourager les personnes qui ont des connaissances au sein de SSAC de partager leurs connaissances.

Et si vous travaillez dans une entreprise concernée, c'est le moment de prendre le micro.

BILL JOURIS : JE ne sais pas si ça compte comme une question. Vous dites que nous ne pouvons rien faire jusqu'à ce que nous ayons un désastre qui nous motive.

ROD RASMUSSEN: C'est dans le cas de .ZIP. Nous avons mené tout le processus, toutes les barrières ont été franchies et maintenant c'est en live et personne n'est mort. C'est terrible, en fait la barre que nous avons fixée c'est : y aura-t-il mort d'être humain ? Mais quel levier ou mécanisme doit-on activer ?

Vous savez quoi faire, il faut donc le retirer de la zone racine. Mais à l'avenir cela sera peut-être un sujet intéressant. Il faut avoir une meilleure idée de ce que sont les préoccupations.

Ici, nous disons que voilà, nous en avons parlé il y a 10 ou 15 ans, maintenant que les gens voient les choses, peut-être qu'il faudrait être en mesure de voir ce que les gens voient. Alors peut-être que c'est là que vous pouvez intervenir.

BILL JOURIS : Peut-être qu'il faudrait discuter avec le conseil général ? Il faudrait qu'il y ait quelque chose dans les contrats, donc consulter notre service juridique, il faudrait peut-être que dans les textes il soit stipulé ce qu'il faudrait faire si quelqu'un meurt. En tout cas essayer de se positionner afin de pouvoir avancer rapidement lorsque nous serions frappés par un désastre au lieu de simplement attendre qu'une autorité gouvernementale ou autre vienne vers nous pour nous dire qu'il faut changer les choses qu'on le veuille ou non.

JONATHAN ZUCK : Du point de vue technique, comment pouvons-nous mettre cela en application ?

PETER THOMASON: Je voudrais parler du risque supplémentaire. C'est un problème si vous cliquez sur un lien, que cela aboutit à ZIP et que ce n'est pas ce que vous attendiez. Vous auriez pu aussi avoir quelquechose.com et ça vous redirige quelque part où vous aurez un fichier exécutable.

Donc cela ne se limite pas au domaine ZIP. Dans le domaine ce serait problématique si vous étiez sur la page principale, si vous avez ZIP/, cela n'aurait aucune conséquence. Donc cela a un rôle à jouer si votre extension est .ZIP et c'est tout.

Le cas le plus important d'utilisation malveillante c'est quand on a l'impression qu'il y a un nom de domaine différent. Donc avant le nom de domaine vous pouvez mettre un signe, un symbole @, mettre une extension et cela se complique. Mais cela a été possible même avant le domaine .ZIP. Il y a déjà eu la possibilité d'utiliser @ et puis l'extension.

Je ne dis pas que cela ne doit pas être corrigé, mais je pense qu'il ne faut pas s'inquiéter trop pour ce TLD en particulier. Je ne pense pas que ce TLD soit particulièrement préjudiciable, mais je ne m'exprime qu'en mon nom.

ROD RASMUSSEN: John a la parole.

JOHN LEVINE : Je vais être rapide. Je dois disconvenir, par exemple Microsoft a pris une décision stupide il y a quelques années, vous pouvez créer un fichier exécutable sur Microsoft et vous cliquez dessus et des choses terribles peuvent arriver. Donc tout le raffut sur .ZIP n'est peut-être pas justifié.

Essayer de réaliser de la sécurité à partir des noms, cela n'a jamais fonctionné. Je pense qu'il est raisonnable de dire aux gens que si un logiciel est mal conçu, là il y aura des problèmes. Mais on ne peut pas avoir une liste exhaustive de tous les fichiers. Il peut y avoir des noms de

fichier qui peuvent être problématiques dans d'autres parties du monde sans que nous en ayons connaissance. Il y a d'autres choses qui doivent nous préoccuper.

[Les commentaires sont hors micro]

JUSTINE CHEW: Je pense que je suis d'accord avec ce monsieur, je pense que nous avons déjà dépassé ce stade. Le navire est passé.

GREG SHATAN: Je pense que la plupart des cas mentionnés par Peter ne sont pas ceux qui nous préoccupent dans la mesure où les gens s'inquiètent de quelque chose. Vous voyez une poignée de types de fichiers qui sont en pièce jointe, vous voyez .PPT, .ZIP, et c'est 95 % de ce que vous voyez. Donc heureusement que personne n'a déposé une demande pour .PPT.

Mais c'est peut-être quelque chose que quelqu'un de malveillant pourrait exploiter. Donc on clique sur un fichier .ZIP en pensant avoir accès à un fichier, mais en fait là on est redirigé vers un domaine inconnu.

PATRIK FELTZ : Donc il faut être en mesure de séparer le type de fichier du nom du fichier. Ce sont deux choses différentes. Si vous utilisez une application qui ne peut pas séparer le type de fichier et le nom de fichier, alors le problème n'est pas du côté du TLD mais du côté de l'application que vous avez choisie. Donc c'est une question d'approvisionnement et une

question de la conception de l'application. Vous n'allez jamais empêcher les gens d'envoyer des fichiers ZIP.

WARREN KUMARI: Pour rebondir sur ce que Patrick a dit, sur votre mail vous voyez cela, que c'est un fichier ZIP, cela n'est pas forcément vrai. Vous pourriez dire que voilà, une photo de mon chat. Et cela pourrait être vrai.

Il y a quelque chose qui va poser problème, vous pouvez avoir un email qui vous dirait : allez sur FOOD.NET et quand vous cliquez cela vous emmène vers un domaine malveillant.

JONATHAN ZUCK : Il est possible de construire quelque chose qui ait l'air d'une véritable URL ?

WARREN KUMARI: Oui et non, les exemples qui ont été donnés, URL ou .ZIP il y un UNICODE barre oblique. Mais visuellement cela va ressembler à une URL, mais c'est la même chose pour Microsoft.Com. C'est une question de confusion URL. Tous les navigateurs, tous les emails vous montrent quelque chose en UNICODE, quelque chose de similaire.

ROD RASMUSSEN: Nous arrivons à court de temps, donc il va falloir conclure notre réunion. Comme vous le voyez, ce sont des choses intéressantes.

Nous arrivons à la conclusion de la réunion. Avons-nous le temps pour un autre commentaire ? Pas vraiment, mais je serais heureux de parler après la réunion.

JUSTINE CHEW: Pourriez-vous me dire qui sont les experts des IDN au sein de SSAC ?

ROD RASMUSSEN: Vous en voyez deux auprès de vous.

JUSTINE CHEW: Donc si je peux vous consulter pendant 5 minutes ?

ROD RASMUSSEN: Très bien.

JONATHAN ZUCK : Merci de votre participation et nous avons hâte de participer à vos travaux. Merci.

[FIN DE LA TRANSCRIPTION]