ICANN75 | Réunion générale annuelle – Séance conjointe : ALAC et le SSAC
Dimanche 18 septembre 2022 – 13h15 à 14h30 KUL

YEŞIM SAĞLAM : Cette séance va maintenant commencer. Veuillez lancer l'enregistrement. L'enregistrement est commencé.

Bonjour, bienvenue à la séance conjointe ALAC-SSAC. Je m'appelle Yeşim Salam et je suis chargée de la participation à distance pour cette séance. Veuillez noter que cette séance est enregistrée et qu'est régie par les normes attendues de comportement à l'ICANN.

Pendant cette séance, les questions ou commentaires soumis sur le chat seront lus à haute voix s'ils sont soumis dans le bon format, tel qu'indiqué sur le chat. Si vous participez via audio, à distance, veuillez attendre qu'on vous appelle par votre nom pour activer votre micro sur Zoom. Pour ceux d'entre vous qui sont dans la salle principale, veuillez lever la main sur Zoom et lorsqu'on vous appellera par votre nom, veuillez activer votre micro de table. Pour le bénéfice des autres participants, veuillez indiquer votre nom pour l'enregistrement et la transcription et veuillez parler à un rythme raisonnable.

Les participants en présentiel sont invités à prendre des écouteurs pour écouter l'interprétation. Ils peuvent également utiliser leurs propres écouteurs. Toutefois, veuillez vous souvenir de retirer vos écouteurs lorsque vous allez activer votre micro de table afin d'éviter toute interférence.

Les participants à distance peuvent avoir accès à l'interprétation via la barre d'outils sur Zoom.

Sur ce, je vais maintenant céder la parole à Jonathan Zuck, vice-président de l'ALAC. Merci.

JONATHAN ZUCK : Bonjour à tous, bienvenue après ce déjeuner et bienvenue à mon interaction préférée entre l'ALAC et le comité consultatif sur la sécurité, la stabilité et sa communauté. En effet, on parle beaucoup d'instabilité à At-Large, donc on apprécie votre présence qui témoigne de la stabilité dans la racine. Je suis très heureux de vous avoir avec nous et je pense que nous avons une alliance naturelle entre nous étant donné nos mandats respectifs pour continuer à défendre les intérêts des utilisateurs finaux et essayer de régler les problèmes relatifs à la sécurité et à la stabilité.

Est-ce que Justine est avec nous ? D'accord.

Alors, le premier sujet que nous allons aborder, conformément à l'ordre du jour, est lié aux questions relatives à l'utilisation malveillante du DNS, des questions qui ont été suscitées par la petite équipe de la GNSO sur l'utilisation malveillante du DNS et qui, finalement, revenaient à savoir ce que vous attendez de nous, ce que d'après vous relève du mandat de la GNSO par rapport à nos procédures et processus par rapport à l'utilisation malveillante du DNS. Ceci a donné lieu à plusieurs idées, concepts et récemment, ces deux derniers jours, une réponse préliminaire a été élaborée pour répondre à ces questions.

Et ce que je vais faire, c'est un petit peu m'avancer pour écouter d'abord la présentation du SSAC, puis allumer mon ordinateur pour voir quelles sont les réponses de Justine à ces questions. Donc on va laisser la parole aux membres du SSAC et avoir ensuite la conversation sur les questions relatives à l'utilisation malveillante du DNS, parce qu'il semblerait qui va y avoir à l'avenir une feuille de route par rapport à l'utilisation malveillante du DNS. Mais en tout cas, on va écouter d'abord la présentation du SSAC.

ROD RASMUSSEN : Merci Jonathan et félicitations pour votre élection. Merci à l'ALAC de nous avoir invités de nouveau. Merci de nous consacrer ce temps. Et effectivement, nous avons un intérêt mutuel à protéger,

les intérêts des utilisateurs finaux, donc c'est toujours une très bonne chose de se retrouver.

Je ne sais pas si Andrei voulait intervenir et nous dire quelques mots. Je suppose qu'il est en ligne. Est-ce qu'Andrei veut intervenir ?

ANDREI KOLESNIKOV : Bonjour, je suis Andrei Kolesnikov. Merci, Rod, de m'avoir laissé la parole.

ROD RASMUSSEN : Oui, pas trop longtemps.

ANDREI KOLESNIKOV : Oui.

Bonjour à tous, bonjour aux membres de l'ALAC, Jonathan, bonjour aux membres du SSAC. Je suis très heureux de vous voir tous.

Conformément à l'ordre du jour, on va commencer par les questions relatives à l'utilisation malveillante du DNS parce qu'en général, ceci nous renvoie à la présentation qu'ont faite les membres du SSAC. On va répondre d'abord aux questions parce qu'en général, à la fin de la réunion, on n'a pas suffisamment de temps pour répondre à toutes ces questions ; c'est pourquoi on a organisé l'ordre du jour de cette manière.

Jonathan semblait vouloir indiquer qu'on commence par la présentation sur les principales thématiques du SSAC parce que c'est la manière habituelle de commencer, mais c'est à vous de décider. Comment est-ce que vous voulez procéder par rapport à l'ordre du jour ? Il serait bon d'entendre les thématiques du SSAC, bien entendu la collision de noms, la sécurité du routage – c'est une autre thématique avec une présentation faite par Russ Mundy – et également sensibilisation, c'est une autre thématique habituelle avec l'accès aux données présentée par Steve Crocker si on a suffisamment de temps avec une discussion et une présentation faite par Rod. Tout cela va dépendre du temps dont on disposera.

ROD RASMUSSEN : Merci Andrei, très heureux de te voir.

On a de très belles images qui vont être assez illustratives et qui vont vous expliquer un peu plus en quoi s'agit le NCAP, projet d'analyse de la collision de noms. Ensuite, les questions relatives à l'utilisation malveillante du DNS, c'est une excellente chose parce que justement, on a parlé hier de la feuille de route, mais on va en parler par la suite.

Alors, à vous Matt.

MATT THOMAS : Merci Rod.

Je suis coprésident du NCAP. Je voulais vous faire une rapide mise à jour par rapport au projet d'analyse de la collision de noms. Je sais qu'on a eu l'occasion avec l'ALAC, il y a un mois environ, de faire une présentation très détaillée par rapport à l'étude du NCAP et je vais aller un petit peu plus loin ici en vous donnant un petit historique et l'état actuel de cette étude.

Comme vous le savez, cela fait maintenant plusieurs années que le NCAP est en cours. Le projet NCAP a été structuré en trois phases distinctes.

D'abord, il y a l'étude 1 qui a été finalisée il y a quelques années maintenant. Il s'agissait d'un recensement approfondi à ce jour de toutes les collisions de noms qui a donné lieu à l'étude 2 qui est en cours maintenant.

L'étude 2 se concentre spécifiquement sur deux principaux objectifs : le premier, essayer de fournir un avis par rapport aux questions du Conseil d'Administration confiées au SSAC par rapport aux problèmes liés à la collision de noms ; et fournir un avis également sur ce qui se passe par rapport à la question spécifique des mails corporatifs depuis la série de 2012. On s'est penché sur ces deux points et on a également effectué d'autres

études de recherche en coopération avec les fournisseurs techniques engagés par l'ICANN qui sont à l'origine des rapports sur la collision à l'issue de la série de 2012.

Nous avons 25 membres, y compris 14 membres des groupes de travail du SSAC. Nous avons 23 observateurs communautaires. Et donc, je vous le disais, on étudie actuellement l'étude 2. Diapo suivante s'il vous plaît.

Il y a eu récemment deux grandes publications qui émanent du groupe de travail NCAP soumises à commentaires publics. D'abord, étude de cas sur les chaînes de collisions par rapport à corp, home et mail. Et deux chaînes supplémentaires ont été ajoutées parce qu'au moment où l'étude a été faite, on avait reçu plus d'un million de requêtes par jour pour les serveurs racine A et J, ce qui a donné lieu à une étude des données DNS vues par le serveur racine pour ces chaînes de collision et la manière dont elles ont évolué au fil du temps. Ceci nous a donné un peu plus d'informations par rapport au travail qu'on a effectué et pour faire avancer un petit peu nos conclusions et cela nous a aidés également à comprendre la manière dont les changements dans l'écosystème du DNS ont évolué avec le temps en raison de facteurs élémentaires, notamment l'évolution du protocole Internet.

Première chose, une étude de perspectives pour les requêtes DNS pour les domaines de premier niveau non existants. De quoi s'agissait-il ? Comprendre les implications des données DNS qui peuvent être collectées et analysées à des fins d'évaluation de risque de collision de noms, ce qui nous a permis d'avoir une bonne idée pour essayer d'avancer pour voir comment ces mesures de données peuvent être utilisées pour évaluer les risques et quelles sont les sauvegardes qu'il faut appliquer lorsqu'il s'agit de ce type de mesures. Diapo suivante s'il vous plaît.

Quelles sont nos principales conclusions ? Vous voyez une liste à l'écran. La principale conclusion, c'est que la collision de noms continue de représenter un problème majeur et croissant. Et cette étude de cas le démontre. Cette étude de cas nous montre bien que ce qui est à l'origine de cette collision de noms qui continue de provenir des problèmes identifiés lors de la série de 2012 dans le rapport lorsque les protocoles de découverte de service DNS et les listes de requêtes de suffixe continuent de constituer un problème.

Il y a un certain nombre de choses qu'on a pu élaborer, notamment les mesures de diagnostic critique. Il s'agit d'outils qui permettent de nous aider à évaluer, d'un point de vue quantitatif, les risques que les collisions de noms peuvent

potentiellement représenter. Et à cela s'ajoute l'étude qui nous permet de fournir et de mettre en place ces sauvegardes pour évaluer les risques lorsqu'on regarde un certain nombre de choses dans la hiérarchie DNS.

Les principales conclusions qu'on voit dans cette étude, c'est qu'il s'agit d'une question de volume et de diversité et que quand ces deux vecteurs augmentent, la difficulté à évaluer la menace et les risques que représente la collision de noms augmentent aussi. Cette recherche, en coopération avec d'autres secteurs et groupes communautaires, a permis d'identifier des opportunités pour les plateformes CDM, telle que la plateforme ITHI, pour aider les candidats lorsqu'ils présentent leur candidature ou lorsqu'ils vont présenter leur candidature pour la prochaine série. Et ceci permet d'aider les candidats avant de soumettre leur candidature. Cela va aider la communauté parce que cela leur permet de savoir, avant de se lancer dans le processus de candidature, certaines informations préliminaires concernant la collision de noms. Diapo suivante s'il vous plaît.

Alors, qu'en est-il de ces CDM, mesures de diagnostic critique ? Pour ceux d'entre vous qui se souviennent du rapport JAS par rapport à la série de 2012, vous vous souviendrez que ces mesures de diagnostic critique ressemblent étrangement à ce qui a été révélé par ce rapport.

Le volume des requêtes, ce n'est pas un indicateur qui, à lui seul, peut démontrer la menace. Il y a d'autres mesures qui sont importantes, par exemple la diversité sous différents aspects, par exemple la diversité en termes d'adresses IP, la diversité en termes de distribution ASN, ka diversité en termes de types de requête ; tout en combinaison avec tous ces éléments nous permet de décrire l'impact potentiel ou la menace potentielle de chaînes de collision. Bien entendu, tous ces éléments ne sont pas exhaustifs, il y a d'autres aspects qualitatifs à prendre en considération et cela devrait se faire au cas par cas en fonction des chaînes.

Où en est le groupe de discussion sur le NCAP actuellement ? On essaie de mettre en place les résultats de l'étude 2, on essaie de mettre en place un flux de travail systématique qui permet au Conseil d'Administration d'avoir un système en place pour évaluer la collision de noms. Et cela s'accompagne par l'avis relatif à l'étude 2 et son rapport. Nous tentons de soumettre ce rapport pour commentaires publics d'ici le dernier semestre 2022.

Pour ceux d'entre vous qui souhaitent contribuer ou nous rejoindre, sachez qu'il y a une réunion du groupe de discussion du NCAP mercredi. Il y a également une liste de diffusion ; vous pouvez vous y inscrire pour suivre nos discussions. Donc surtout,

n'hésitez pas à venir nous rejoindre. L'étude 2 va être publiée sous peu, mais vous êtes tout à fait les bienvenus à participer.

JONATHAN ZUCK : Merci Matt pour cette présentation. Effectivement, c'est un sujet qui intéresse beaucoup notre communauté. On avait une discussion au CPWG sur ce rapport, mais peut-être que c'est quelque chose de nouveau pour les gens ici présents dans la salle.

Je ne sais pas s'il y a des questions dans la salle. N'hésitez pas à lever la main et veuillez me dire s'il y a des questions sur Zoom parce que je ne les vois pas l'écran. Imaginez que le résultat de cela, c'est un système de score pour calculer les risques qui permettrait un classement. Ou est-ce que vous pensez plus à une série complexe d'évaluation de risque qui serait utilisée en coopération avec des efforts d'atténuation par exemple ? À quoi pensez-vous que cela va rassembler ?

MATT THOMAS : Excellente question. Pour répondre à votre question, je pense plutôt à la deuxième option. Il y a une composante fondamentale sur laquelle le groupe s'est mis d'accord : comprendre d'abord le risque pour essayer d'en établir un profil et pouvoir avancer. C'est la meilleure voie à suivre pour le Conseil d'Administration pour faire face à ce problème.

Ce dont on a parlé au groupe de travail, c'est essayer de fournir ces sauvegardes, ces lignes directrices, et avoir un système pour essayer de mettre en place ce système.

JONATHAN ZUCK : Et est-ce que vous pensez que corp et home, ça va être suffisamment atténué pour être délégué ?

MATT THOMAS : Si vous voulez mon opinion personnelle – mais je vous invite à consulter l'étude elle-même –, je n'en suis pas sûr.

JONATHAN ZUCK : Très bien.

Y a-t-il d'autres questions ? Est-ce qu'on a des questions sur Zoom ? Très bien, alors à vous Rod.

ROD RASMUSSEN : Bon, pas de questions, très bien. Diapo suivante s'il vous plaît.

Le routage, on a parlé auparavant, mais là, on a une présentation plus détaillée. Russ, est-ce que vous pouvez nous faire cette présentation ? Russ est à distance. Est-ce que vous pouvez nous faire cette présentation, Russ ?

RUSS MUNDY : Bonjour à tous, j'espère que vous avez eu une bonne pause-déjeuner. Bonjour à tous dans la salle et à tous ceux qui nous accompagnent en ligne. Je vais vous faire cette présentation sur SSAC121. Comme Rod l'a dit, nous avons eu cette présentation juste avant qu'elle soit publiée. Grâce à notre personnel de soutien à l'ICANN, nous avons maintenant une série d'éléments qui nous permettent de bien structurer ce document. Peut-être que certains d'entre vous auront lu ce document. L'idée aujourd'hui, c'est de vous donner un aperçu de ce document. Surtout, n'hésitez pas à lever la main ou à intervenir si vous avez des questions à tout moment de cette présentation.

Voici l'aperçu de ce document qui est divisé en cinq thématiques que vous voyez ici à l'écran. Diapo suivante s'il vous plaît. Cette image en particulier provient directement du document en question. De quoi s'agit-il ? Il s'agit d'une description. On a très peu de temps pour vous montrer cette image. Mais vous voyez ici une illustration. J'espère que vous comprenez : c'est un exemple où un client C fait une recherche sur son portable et pose la question « Où se trouve www.exemple.net ? » Cette requête DNS passe par le résolveur DNS. Et comment cela se fait-il ? En passant par ce que vous voyez en bas, AS1, AS2, AS3, pour aller jusqu'au résolveur D. Le résolveur D fait ensuite ce qu'on appelle le récursif sur le DNS pour aller jusqu'au serveur faisant autorité, c'est-à-dire pour obtenir une réponse à cette question. Et dans ce cas-là,

le résolveur D du DNS passe par le serveur faisant autorité A et ceci passe par les systèmes autonomes 3 et 6. Et là encore, en bas de cette image, vous voyez comment ces paquets sont traversés et vous voyez là donc une illustration du protocole DNS de lui-même. La réponse du serveur DNS A un est ensuite renvoyée au D puis au client C. Et on revient donc par AS3, AS2 et AS1.

C'est un exemple, parce que si vous y réfléchissez pendant quelques minutes, c'est impressionnant de voir que tout cela se passe. Et cela se passe avec toutes les requêtes DNS et tout cela passe par le serveur DNS et par le routage. Passons à la diapo suivante s'il vous plaît.

Ici, c'est un exemple d'un type d'attaque. Dans ce cas, l'attaque se déroule à AS1. Quand le client envoie sa requête pour arriver au résolveur D, cela n'arrive pas au résolveur D, mais si c'est le cas, on reçoit une réponse plus rapide du résolveur malveillant en bas de la page et cela se fait par un détournement de routage. Si vous voyez l'adresse de retour, elle est différente que ce qui proviendrait du serveur légitime faisant autorité. Vous voyez en haut que l'adresse est différente et c'est le résultat du détournement. Diapositive suivante.

Y a-t-il des questions que vous souhaiteriez poser ? Car ce sont des concepts importants à comprendre. Bien.

Ce n'est pas le seul moyen donc que le détournement de routeur peut prendre. Diapositive suivante.

Le détournement de routage le plus connu et qui peut entraîner des résultats à fort impact, c'est ce qui est appelé MyEtherWaller/Route53. C'est un groupe de criminels ; dans ce cas, nous ne savons pas qui, ils n'ont jamais été identifiés à ma connaissance, et ils ont été en mesure de procéder à un détournement très similaire à ce que nous avons vu à la diapositive précédente. Ce qu'ils ont fait pour détourner la route, c'est le service DSN Route53 géré par Google. Avec ce DNS malveillant, ils ont été en mesure de voler 150 000 $ en environ deux heures.

L'autre impact, c'est que les malfrats ont pu, grâce à ce détournement, procéder au vol et bien d'autres personnes essaieront de faire la même chose. Évidemment, le montant volé de 150 000 $ est considérable en deux heures, mais en plus de cela, ils ont éjecté tous les autres utilisateurs du service DNS Route53 pour toutes les requêtes DNS sauf pour MyEtherWaller, toutes les requêtes retournent un *Serve Fail*.

Je vois que nous avons une question. Oui.

HADIA ELMINIAWI : Lorsqu'il y a cette attaque BGP, est-ce que cela a été identifié comme étant une attaque métrique ou un incident DNS ? Comment l'appelleriez-vous ?

RUSS MUNDY : Je dirais que ce sont les deux ; les deux principaux protocoles sont impliqués. La première attaque s'est déroulée sur le système de routage BGP, mais pour réaliser cette attaque, ils ont dû donner des réponses malveillantes de DNS. Et les requêtes ont reçu des réponses incorrectes, cela a posé un problème au niveau du DNS depuis de nombreuses années. Donc, les gens qui n'utilisent pas de système de noms de domaine de DNSSEC sont très vulnérables aux attaques.

Est-ce que c'est clair ? Est-ce que c'est une réponse compréhensible ?

HADIA ELMINIAWI Merci.

ROD RASMUSSEN : Il y a une question dans le chat.

RUSS MUNDY : Merci Rod, je ne l'avais pas vue. Le diagramme précédent. Bien.

L'AS4 est aussi impliqué. Ce n'est pas sûr, mais c'est probablement le cas. Le système de routage lui-même est conçu pour être un ensemble d'informations qui ont été décrites par

certaines personnes comme étant des rumeurs entre personnes qui se font confiance mais qui ne devraient pas se faire confiance. Il faudrait donc améliorer la sécurité. Les vulnérabilités au niveau du BGP ont lieu depuis de nombreuses années.

Est-ce que c'est une réponse suffisante à la question posée dans le chat ?

ROD RASMUSSEN : Il y a Sander qui a une question.

SANDER STEFFANN : Vous avez dit qu'ils ont retourné *Serve Fail* pour toutes les requêtes. J'imagine que si les données appropriées avaient été données pour tous les autres domaines, cela aurait été différent.

RUSS MUNDY : Vous avez peut-être raison, ce sont des spéculations, mais en réalité, si vous procédez à ce type d'attaque et que vous vous rendez moins visibles, il faudra plus de temps pour que ce qui se passe soit identifié, alors probablement que oui.

Est-ce qu'il y a d'autres questions à ce stade ? Bien.

JONATHAN ZUCK : On ne dirait pas.

RUSS MUNDY : Merci Jonathan. Passons à la diapositive suivante s'il vous plaît. Bien.

Ici, nous avons un ensemble de diapositives plus denses et contextualisées. Ce que nous avons identifié ici, c'est qu'il y a un grand nombre d'endroits où ces interactions peuvent se dérouler et il y a beaucoup de vulnérabilités et elles pourraient être améliorées si tous les mécanismes de sécurité étaient en place. Par exemple, il y a des mécanismes pour identifier le serveur qui fournit une réponse à une requête. Très peu de résolveurs utilisent cela. Le DNSSEC permettrait cet empoisonnement. Mais parmi les clients, la majorité ne procède pas à la validation du DNSSEC. Si c'était le cas, la requête n'arriverait pas au résolveur récursif.

Vous voyez qu'il y a un grand nombre d'endroits où on pourrait mettre en place des mécanismes de renforcement de la sécurité. La technologie est disponible pour cela, mais cela n'est pas fait actuellement.

Est-ce qu'il y a des questions sur cette diapositive ou sur son contenu ? Bien. La diapositive suivante s'il vous plaît.

Avec la séquence de cette attaque en particulier, une des raisons pour lesquelles nous avons choisi cette attaque à titre d'exemple, soit ce que font les malfrats dans la réalité, c'est pour vous permettre de voir la séquence des événements de façon claire. Et le résultat, comme vous le voyez dans la partie conséquences,

c'est un vol considérable perpétré par quelqu'un, et un grand nombre de personnes qui utilisaient le DNS Route53 ont connu une panne de serveur pendant plusieurs heures. Diapositive suivante.

La partie du document qui porte sur les possibilités d'amélioration de la sécurisation du système de routage, c'est le sujet qui nous concerne. Il y a eu beaucoup de questions qui ont été posées sur l'amélioration des processus internes. La sécurisation du routage porte sur davantage de choses que sur les aspects techniques. Ce que l'on entend surtout, c'est la sécurité du protocole de passerelle frontière. Il y a des faiblesses et des centaines d'attaques tous les jours.

Il faut savoir si c'est une attaque ou une erreur. Parfois, on peut se dire : « Oups, c'est quelque chose que je n'aurais pas dû faire. », mais en réalité, dans la plupart des cas, on ne peut pas faire la distinction entre ce qui est intentionnel et non intentionnel. Ce peut être difficile à déterminer. Il y a un indicateur très subjectif et c'est celui de la rapidité avec laquelle le problème peut être corrigé. Si c'est une erreur, on peut le corriger aussi rapidement que possible, tandis que si c'est une attaque agressive, les gens vont tout simplement disparaître et ils ne vont pas reconnaître qu'il y a eu quoi que ce soit qui s'est déroulé. On ne peut pas vraiment distinguer les deux.

Un autre aspect important dans le renforcement de la sécurité, c'est une politique de routage exacte pour vos opérations. Si votre opération est principalement une opération [INC], c'est une chose, tandis que si vous avez une opération centrée sur le DNS, vous aurez sans doute des fournisseurs de services qui réalisent le routage pour votre compte et il vous faudra savoir que leurs politiques sont exactes et maintenues.

Un autre aspect important, c'est la robustesse des opérations. Nous parlons de plusieurs éléments dans le document. Le premier point que nous soulignons se rapporte à un groupe d'opérateurs qui ont créé ce qui s'intitule MANRS, et il y a beaucoup de principes. Ce sont des principes d'accord mutuel sur la sécurité de routage. Ce sont donc les pierres angulaires de l'amélioration de la robustesse du système de routage. Diapositive suivante.

En ce qui concerne les aspects techniques BGP, il y a ces registres de routage. Ce sont des bases de données essentiellement qui fournissent un mécanisme afin que les opérateurs puissent placer leurs données dans un endroit où elles puissent être partagées et être utilisées. Il y a de nombreuses limitations. Il y a un grand nombre de registres de routage et il y a des informations contradictoires entre les registres de routage, donc il y a une absence de robustesse. La diapositive suivante s'il vous plaît.

En ce qui concerne l'infrastructure de gestion de clés publiques, c'est ce qui permet au récepteur de savoir si les informations sont émises de façon autorisée. Nous passons à la diapositive suivante, sauf s'il y a des questions.

Je vais passer en revue cette diapositive assez rapidement. C'est une façon différente d'illustrer ce que nous avons vu précédemment. C'est une approche plus détaillée du renforcement de la sécurisation. Les opérateurs d'infrastructure, qu'il s'agisse d'infrastructure de DNS ou autre, doivent surveiller les systèmes externes et internes. Il faut qu'il y ait une coordination avec tous les autres opérateurs. Il faut une coopération établie et il faut pouvoir savoir qui contacter en cas de problème. Il faut suivre les principes prescrits ; c'est fortement suggéré. Diapositive suivante s'il vous plaît.

Aujourd'hui, il y a des anomalies de routage quotidiennement. Il y en a des centaines, parfois des milliers par jour. Et pour améliorer la robustesse de la sécurité de routage, il faut la collaboration de la communauté entière. Beaucoup de personnes peuvent contribuer, surtout celles qui savent ce qui peut être fait pour améliorer la sécurité.

Nous avons une question qui est posée. On dirait un arbre et une échelle. Veuillez poser votre question.

SIVSUBRAMANIAN MUTHUSAMY : Pouvez-vous m'entendre ?

ORATEUR NON-IDENTIFIÉ : Oui

SIVSUBRAMANIAN MUTHUSAMY : On nous dit que l'organisation doit surveiller les racines. Est-ce qu'il faut identifier les données compromises ? Les routes, peuvent-elles être surveillées ? Y a-t-il un processus à cet effet ?

RUSS MUNDY : Il n'y en a pas. Il n'y a pas de processus unique ou simple. Il y a des systèmes de surveillance. Chaque opérateur qui a élaboré un système, qu'il s'agisse de DNS ou de routage, doit personnaliser sa surveillance selon ses besoins pour savoir si son système subit des abus au niveau interne ou externe. La coordination entre les opérateurs est essentielle. Il faut cette coordination entre clients et opérateurs et il faut savoir qui contacter. Le routage sur Internet, il est massif, il implique des milliers d'activités et selon moi, il ne pourrait pas y avoir un système de surveillance unique.

SIVSUBRAMANIAN MUTHUSAMY : Pourrais-je répondre ?

Les différents opérateurs ont différents niveaux d'expertise. Certains ont l'intention de sécuriser leur routage, mais d'autres n'ont peut-être pas l'expertise nécessaire, ne savent pas

comment le faire. C'est pour cela qu'un organe tel que le MANRS doit pouvoir identifier les problèmes et tous les problèmes de malveillance. C'est ce que je voulais suggérer.

RUSS MUNDY : Il y a beaucoup d'exemples de capacité où vous n'avez pas besoin de dépenser beaucoup d'argent. C'est une décision commerciale que vous devrez prendre. Nous n'avons pas de recommandations à l'endroit du Conseil d'Administration dans le document, mais pour les opérateurs, ils ont acquis les connaissances dont ils ont besoin pour pouvoir efficacement surveiller et répondre aux attaques de routage et les prévenir. Tout cela implique une infrastructure qui doit être mise en place.

Je dois dire que ce document a une annexe où il y a une liste considérable relative aux questions sécuritaires plus que dans tout autre document. Il y a beaucoup d'informations dans l'annexe du document. Ces informations seront utiles pour que les gens puissent trouver des réponses.

Je crois que c'est la dernière diapositive.

JONATHAN ZUCK : Merci Russ. C'est un document intéressant pour voir quelle est l'intersection entre l'organisation ICANN et la communauté du point de vue de l'élaboration des politiques. Et tout ce qui peut être ajouté ici nous montre qu'il faut essayer de penser de

manière proactive, traiter cette question sur la base de la communauté et essayer de mettre à profit les canaux de communication dont on dispose pour essayer de faire parvenir ce document à la communauté des opérateurs. Mais est-ce que c'est l'organisation ICANN qui peut se charger d'atténuer les risques ou la communauté ?

ROD RASMUSSEN : On va faire un briefing au Conseil d'Administration sur cette question. Mais effectivement, c'est l'une des choses qu'on aimerait voir, que l'organisation ICANN soit derrière cela et diffuse ce document auprès de la communauté des opérateurs aussi largement que possible, parce que cela concerne le DNS. Il faut que les opérateurs soient absolument conscients de cela. Là entrent en jeu les connaissances, mais plein d'autres choses aussi et il serait utile pour la communauté DNS de savoir que ce genre de chose se produit et qu'il y a un renforcement de capacités à ce niveau-là.

Mais ceci, je le répète, c'est une discussion qu'on veut avoir avec l'équipe communication, avec l'organisation ICANN. Mais ce qu'on voulait dire ici, c'est que vous avez, vous aussi, une certaine influence pour diffuser ces informations. Il faudrait essayer absolument de sensibiliser par rapport à cela.

JONATHAN ZUCK : Effectivement, je vais en lire plus à ce sujet après cette séance parce que c'est quelque chose de très important. Bien.

Passons à la présentation de Julie très rapidement.

ROD RASMUSSEN : Je vais intervenir avant de céder la parole à Julie puis à Steve Crocker pendant quelques minutes qui va nous parler du SSAD, système normalisé d'accès et de divulgation. Et ensuite, on pourra se concentrer sur la question qui vous intéresse le plus.

Julie, allez-y brièvement.

JULIE HAMMER : Merci Rod.

Comme la plupart d'entre vous le savent, nous avons une enquête de compétences qui définit le type de compétences qu'on recherche au SSAC. Et bon nombre de nos membres ont utilisé cette liste de compétences pour intégrer un certain nombre de nouveaux membres, faire une auto-évaluation de nos membres et une mise à jour de leurs compétences. Diapo suivante.

On l'utilise aussi pour identifier les lacunes en termes de capacités qui font que l'on soit à la recherche de nouveaux membres, en particulier les lacunes en termes de capacités et les

capacités qu'on recherche chez les nouveaux membres. Et on essaie d'accroître également la diversité dans un certain nombre de domaines, en particulier la diversité géographique avec de nouveaux membres provenant de l'Afrique, de l'Amérique latine et de l'Asie-Pacifique, et également de nouveaux membres qui pourraient avoir un bagage universitaire et avoir des compétences dans le domaine de l'analyse. Diapo suivante.

Si vous avez ces compétences, si vous connaissez quelqu'un qui a ces compétences dans ces domaines surtout, n'hésitez pas à nous contacter [inaudible] à faire de la sensibilisation au cours des prochains mois, jusqu'au mois de mars-avril. Et d'ici là, on va analyser toutes les candidatures qui seront soumises au SSAC avec un intérêt tout particulier vis-à-vis des candidatures qui réunissent ces critères. Surtout, n'hésitez pas à consulter cette liste de compétences qu'on recherche, c'est sur notre site Web. Et tous les candidats réunissant ces critères sont invités à nous contacter. Toute personne intéressée peut contacter Rod, moi-même ou tout membre du SSAC.

Merci.

ROD RASMUSSEN : Merci Julie.

Y a-t-il des questions ? N'hésitez pas à intervenir. Sinon, on va continuer à avancer.

Steve Crocker, est-ce que vous êtes là pour nous en dire un peu plus par rapport à où nous en sommes par rapport au système SSAD ?

STEVE CROCKER : Oui, toujours prêt. Je crois qu'on a quelques diapos à projeter, mais je vais vous donner un aperçu un peu plus général de la situation, parce que je ne suis pas sûr que tout le monde soit au courant.

L'ICANN se débat avec le problème WHOIS ou le problème d'enregistrement des données depuis pas mal de temps maintenant. Quelle est la situation actuelle ? Il y a une version légère ou moins détaillée qui s'appelle la version WHOIS qui essayait de déployer aussi rapidement que possible un système de ticketing qui renvoie les requêtes aux bureaux d'enregistrement. Il y a très peu de contenu pour ce qui concerne la description de requêtes ou la manière dont les bureaux d'enregistrement la gèrent.

Ensuite, il y a une autre partie où la GNSO et le groupe de travail sur les politiques accélérées de la GNSO ont essayé de définir ce que va constituer la révision aux spécifications temporaires et

éviter toute spécification par rapport aux règles pour l'accès aux données non publiques. Et il y a encore un long chemin à parcourir parce que même si on a beaucoup fait, on continue à voir le problème par rapport au fait de savoir qui sont les utilisateurs, quels sont leurs besoins. Et ces discussions ont été ignorées, donc on est dans une situation compliquée. Voilà un petit résumé de la situation.

ROD RASMUSSEN : Merci, très bien.

Y a-t-il des questions à l'attention de Steve, à mon attention ou à d'autres membres du SSAC par rapport à la situation actuelle ?

JONATHAN ZUCK : Où on en est tout court et non pas seulement par rapport au SSAD.

Si vous le permettez, j'aimerais faire intervenir Justine… Ah, non, excusez-moi, Alan, je n'avais pas vu votre main levée.

ALAN GREENBERG : Merci beaucoup. Très brièvement, j'aimerais remercier le SSAC et Steve. Steve a effectué un travail extraordinaire pour essayer de forcer les différents groupes à se concentrer sur les problèmes réels. J'apprécie les efforts de Steve et toute l'énergie qu'il y a consacrée.

STEVE CROCKER : Merci Alan. Laissez-moi vous dire que je pense que ce serait pertinent et opportun pour l'ALAC de se manifester clairement par rapport à ce dont on a besoin. Effectivement, on a participé activement à ce niveau-là et chacun des groupes de travail a fixé ses propres règles. Mais la situation réelle, c'est que les choses n'avancent pas de manière efficace. L'ALAC, c'est l'une des principales organisations qui représentent les gens qui ont supposément besoin des données. Et les gens qui ont les données, ce sont les parties contractantes à l'ICANN, les opérateurs de registre et les bureaux d'enregistrement. Et, sans vouloir les critiquer, ces parties contractantes – et on le comprend bien – se concentrent pour essayer de minimiser les risques et les dépenses. Mais ils font peu de cas par rapport aux gens qui ont besoin de ces données à des fins légitimes. Ils sont prêts à le faire, mais ils ne vont pas passer beaucoup de temps à essayer de résoudre ces problèmes et essayer de faire avancer les discussions sur cette question.

ROD RASMUSSEN : Oui, ça, c'est l'opinion personnelle de Steve sur la question.

STEVE CROCKER : Oui, tout à fait.

ROD RASMUSSEN : Ce n'est pas le la position officielle du SSAC sur cette question, je précise. Mais il y a effectivement beaucoup d'efforts en cours, mais comme Steve l'a dit, il y a des intérêts conflictuels. Et dans

toute situation de ce type avec des conflits ou des intérêts conflictuels, c'est difficile de se mettre d'accord par rapport à l'accès aux données. On essaie de se concentrer pour faire avancer les choses, mais cela ne fonctionne pas pour l'instant. On va continuer à adopter cette approche et je suis sûr que vous allez faire de même.

Ce qui nous amène à la question du DNS, n'est-ce pas ?

JONATHAN ZUCK : Oui, tout à fait. Pour nous faire un bref résumé par rapport aux réponses de la petite équipe sur l'utilisation malveillante du DNS… Excusez-moi, je n'avais pas vu la main levée de Sébastien sur Zoom.

SÉBASTIEN BACHOLLET : Merci.

Steve, je voulais revenir à cette question. Et pourquoi ? Parce que c'est bien beau demander à tous les participants de la communauté ICANN de participer – et j'espère que c'est bien la position de l'ensemble du SSAC et non pas la position personnelle de Steve – mais moi, le problème que j'ai par rapport à cela, c'est que si on ne règle pas le problème de la personne physique et de l'organisation, nous, en tant qu'utilisateur final, on a un problème et moi, je parle en tant qu'Européen. Je ne comprends pas pourquoi il est clairement stipulé dans le RGPD que ce sont les

données des personnes physiques et non pas des personnes morales qui doivent être publiées. Donc si on peut essayer de résoudre d'une autre manière cette question, mieux ce sera. Mais je ne vois pas comment un utilisateur final qui demande accès aux données, ce doit être naturellement accessible. Merci.

JONATHAN ZUCK : Merci Sébastien, c'est une discussion en cours, c'est sûr. Et effectivement, le RGPD permet la distinction mais ne la rend pas obligatoire, cette distinction entre personnes physiques et personnes morales. Ce sont des discussions en cours.

ROD RASMUSSEN : Très rapidement.

D'un point de vue technique, c'est quelque chose qu'on peut régler facilement, mais ce sont des questions épineuses d'un point de vue juridique. Et on n'a aucun problème pour dire que d'un point de vue technique, on peut régler ce problème très facilement.

JONATHAN ZUCK : Très bien.

Alors, allez-y parce qu'on veut traiter maintenant la question du DNS.

HADIA ELMINIAWI : Très brièvement, par rapport à l'aspect technique, on nous a toujours dit que pendant l'EPDP, on ne faisait pas cette distinction parce qu'on avait peur des erreurs, parce que les solutions techniques à cela sont encore dangereuses et n'offrent aucune garantie.

ROD RASMUSSEN : Là, je parle de préserver les données, je ne parle pas de machine qui pourrait faire automatiquement la distinction entre personnes physiques et personnes morales. C'est de cela que je parle.

JONATHAN ZUCK : Oui, discussion intéressante, merci.

On revient au premier point de notre ordre du jour et Justine a eu la gentillesse de me soumettre le résultat de la petite équipe de la GNSO sur l'utilisation malveillante du DNS. Et elle se trouvait dans la salle, donc je vais lui laisser le soin de nous présenter les résultats de ces questions.

JUSTINE CHEW : Vous me prenez un petit peu de court, Jonathan. Merci. Je ne sais pas quelle casquette je dois mettre maintenant. Vous savez, je suis un peu perdue.

En termes de résultats de la petite équipe du conseil de la GNSO sur l'utilisation malveillante du DNS, il y a eu une séance ce

matin… C'était aujourd'hui ou hier ? Hier, pardon, et le rapport en est probablement à la dernière étape, il est encore en cours d'élaboration, mais il y a quatre recommandations qui ont été soumises. Les quatre recommandations sont, d'après moi, d'ordre général, c'est-à-dire qu'elles répondent à des objectifs de haut niveau.

On a eu une réunion avec la GNSO et j'aimerais avoir le retour des gens pour voir si ces recommandations sont suffisamment spécifiques et satisfaisantes. Mais je voulais dire que dans la séance de la GNSO où Rod et Julie étaient là, vous avez évoqué la possibilité de travailler ensemble et en fait, j'allais parler de cela lors de la prochaine séance, c'est-à-dire la séance de l'ALAC sur les politiques et leur mise à jour.

Par rapport aux procédures ultérieures, vous savez qu'il y a une recommandation pour opérer un effort au niveau de la communauté. Mais ce qui se passe, c'est qu'on a des efforts qui se multiplient ici et là, donc on a différentes parties de la communauté qui font différentes choses. Ce n'est pas une mauvaise chose forcément, mais on retombe dans le même problème : on travaille de manière cloisonnée, on travaille tous de notre côté.

Le commentaire que vous avez fait avec la GNSO aujourd'hui pour prendre la tête de cet effort, pour travailler tous ensemble et réunir tous ces efforts des différentes parties de la communauté, moi, je vous inviterais ou j'inviterais vivement l'ALAC à rejoindre cet effort. Et je suis sûr que l'ALAC va pousser pour que cela ait lieu.

JONATHAN ZUCK : Oui, je pense que la réponse de la petite équipe du conseil de la GNSO a impliqué qu'on modifie un petit peu la conversation et de passer à autre chose. Elle a suggéré le besoin et l'idée d'avoir une feuille de route ; cela jette un petit peu les bases des prochaines étapes. Donc oui, on est tout à fait disposés à participer à ce genre d'effort.

ROD RASMUSSEN : Si vous le permettez, vous et moi, on a déjà eu une conversation hier là-dessus, mais il serait bon d'entendre les autres membres de l'ALAC. Et c'est intéressant d'ailleurs parce que ma vision des choses, c'est qu'il y a une bonne conversation en ce moment à l'ICANN, il y a beaucoup de coordination entre les présidents des différents groupes, mais on peut beaucoup faire. On a beau faire chacun de notre côté, s'il n'y a pas de coordination, vous venez de parler de travail cloisonné, c'est vrai, on a parlé avec le Conseil d'Administration et d'ailleurs, c'était une question du Conseil d'Administration à l'attention de tous pour essayer d'élaborer une feuille de route, une vision, un plan stratégique pour que les

objectifs de haut niveau autour de l'utilisation malveillante du DNS se fassent au niveau de la communauté dans son ensemble.

Donc effectivement, on va essayer de rassembler et de rallier tous ces efforts. On en a parlé avec la GNSO aujourd'hui et effectivement, il y avait beaucoup de gens dans la salle qui semblaient d'accord, surtout avec le rapport de la petite équipe qui va être publié sous peu.

Donc très bien, on peut coordonner les discussions sur cette thématique et notre objectif sera de travailler avec le Conseil d'Administration et avec toutes les autres unités constitutives qui souhaitent mettre en place un projet ou un plan, je ne sais pas bien comment l'appeler, pour traiter les différents points de ce problème. Mais ceci nous oblige tous également à définir ce qu'on essaie de régler, soit ce qui relève du mandat de cette communauté.

Ce qui est important de dire aussi, c'est que pour les choses qui ne relèvent pas de notre mandat, il ne s'agit pas de dire « Ce n'est pas notre problème », mais de dire « Cela relève du mandat de telle et telle autre » et c'est à eux de le régler. Et peut-être qu'à ce moment-là, il faudra voir si c'est notre problème ou pas.

C’est une observation personnelle que je fais, mais voilà un petit peu ce dont on va parler demain et après-demain avec le Conseil d’Administration. On va leur en parler, cela nous semblait pertinent d’en parler avec le Conseil d’Administration, mais il serait bon de voir ce que vous faites, ce que fait le GAC, les différents efforts qui sont déployés au sein de la GNSO ou sein des unités constitutives. Il y a beaucoup de groupes de travail qui travaillent sur cette question ; tous ces efforts, ce serait une bonne chose, mais il faudrait se mettre d’accord au sein de la communauté pour ce faire.

Et un autre grand avantage de cela, c’est montrer que la communauté ICANN, la communauté At-Large, a un plan, des mesures et des résultats pour analyser ce problème, parce qu’il y a beaucoup de gens qui disent : « Aujourd’hui, l'ICANN peut régler ce problème et ne fait rien. » Ce n’est pas vrai, il y a beaucoup de choses qu’on est en train d’essayer de faire, mais il faut pouvoir démontrer le travail qu’on est en train de faire et quelles en sont les résultats.

Voilà un petit peu pour une observation personnelle.

JONATHAN ZUCK : Nous avons fait beaucoup de travail concernant les abus. Il y a un sous-groupe sur l'utilisation malveillante du DNS qui a une réunion. Donc c'est très difficile de fixer le moment d'une réunion pour chacun. Mais le résultat de beaucoup de ces efforts, c'est d'avoir une définition sur ce que constitue l'utilisation malveillante du DNS et ce qui relève de la compétence de l'ICANN.

En ce qui concerne la position d'At-Large, il n'y a pas besoin d'une définition pour améliorer les choses. Si on accepte une définition étroite ou pas, il y a de toute façon du travail à faire. Donc il faut être prudent en ce qui concerne ce que nous [implantons].

Il y a toute la communauté des entreprises qui génère des données. Il y a des données qui sont générées par voie de listes noires. Il y a l'Institut sur l'utilisation malveillante du DNS. Il y a donc cet accent qui est mis sur l'utilisation malveillante du DNS et l'idée de détournement est maintenant mise à l'écart du domaine de compétence de l'ICANN. Il y a un grand chevauchement entre les bureaux d'enregistrement et les fournisseurs d'hébergement. Des domaines sont vendus à des entités telles que Wix, Squarespace et il se peut que ces superviseurs d'hébergement puissent peut-être gérer les questions d'utilisation malveillante de domaine. Mais il faudrait peut-être créer une communauté au sein de l'ICANN. Pour revenir à ce que vous disiez, si on lance la balle, il n'y aura peut-être

personne pour l'attraper et nous n'aurons peut-être pas géré le problème.

Je voulais voir si quelqu'un souhaiterait s'exprimer à ce sujet. Je ne vois pas de carte dans la salle, je ne vois pas de main virtuelle. Je vous encourage tous à consulter le rapport de la petite équipe GNSO sur l'utilisation malveillante du DNS.

Nous nous focalisons sur cela aussi dans nos réponses à ces questions. Il ne faudrait pas exclure les autres thématiques. Il y a aussi d'autres thématiques tels que les enregistrements en vrac. Il y a des questions qui ont été soulevées, alors il faut veiller à ce que nous puissions répondre aux questions qui sont posées. Enfin, nous devons travailler avec vous pour établir une feuille de route.

GABRIEL ANDREWS : Je ne sais pas à qui il faut poser cette question, à vous ou aux autres collègues du SSAC dans la salle.

En ce qui concerne la complexité du marché de détail, les intérêts commerciaux, les différents services, je me demande dans quelle mesure il existe des systèmes qui auraient été mis en place pour établir les rôles et les responsabilités. Est-ce qu'il y a eu une mise à jour de ces rôles et responsabilités ? Je ne sais pas ce que pensent les gens de cela.

ROD RASMUSSEN : On parle d'un marché d'infrastructures, d'une cartographie du marché. Je ne sais pas si l'ICANN a réalisé cela. Je crois que les choses deviennent complexes très rapidement. Il faut comprendre quel type de compromis il est nécessaire de faire. C'est une décision qui dépend des différents niveaux de connaissances. En fonction des connaissances que l'on a, on va choisir la trajectoire. Il y a des gens qui s'occupent de la cartographie et il faudrait peut-être établir une cartographie qui traiterait uniquement des abus. C'est peut-être une question qui relève du secteur académique. Il faudrait peut-être déployer cet effort de planification et de coordination car il y a toujours des malentendus fondamentalement sur ces sujets.

JONATHAN ZUCK : C'est vrai. Il faudrait qu'il y ait des limites à ce qui est considéré comme le domaine de compétence de l'ICANN.

Le personnel me dit que nous avons dépassé le temps imparti. Veuillez vous joindre à moi pour remercier nos intervenants. Nous continuerons notre conversation. Nous avons beaucoup de travail à réaliser ensemble.

**[FIN DE LA TRANCRIPTION]**