COPENHAGUE – Réunion publique du SSAC
Mercredi 15 mars 2017 – 15h15 à 16h15 CET
ICANN58 | Copenhague, Danemark

PATRIK FÄLTSTRÖM: Est-ce que les membres SSAC peuvent me rejoindre à la table, s'il vous plait ?

Il est 15 h 15 de l'après-midi passé. Finalement, on n'est pas comme d'habitude le jeudi à 8 h 00 du matin même si on a notre café sur la table.

Je m'appelle Patrik Fältström. Je suis président du SSAC (comité consultatif sur la sécurité et la stabilité). Je viens de faire une blague, parce que, souvent ou par habitude, on se retrouve toujours à 8 h 00 du matin le jeudi, et qu'il y a souvent beaucoup plus de personnes à notre réunion. Donc c'est un grand changement pour nous.

Je suis… J'ai des membres SSAC autour de moi, qui ont des emplois différents. Vous voyez les tâches de SSAC et de ces membres, c'est de participer aux séances et d'être actifs, et la réunion de l'ICANN nous permet de faire cela. Donc, je vais présenter les personnes à la table, à gauche. Je vais demander aux personnes donc de se présenter.

ROD RASMUSSEN: Rod Rasmussen, je ne suis pas affilié.

TARA WHALEN: Tara Whalen avec Google.

PATRICK JONES: Patrick Jones.

JAAP AKKERHUIS: Jaap Akkerhuis.

ROY ARENDS: Roy Arends.

GEOFF HUSTON: Geoff Huston, APNIC.

JAMES GALVIN: James Galvin, vice-président et aussi Afilias.

PATRIK FÄLTSTRÖM: Patrik Fältström, président SSAC.

RAM MOHAN: Ram Mohan d'Afilias et liaison SSAC au Conseil.

BEN BUTLER: Ben Butler. Je fais partie un peu de tout, mais je ne suis maître de personne.

WARREN KUMARI: Google.

JOHN LEVINE: John Levine, je suis un petit peu affilié à l'Internet Society.

JEFFREY BEDSER: Jeff Bedser.

GREG AARON: Greg Aaron.

ROBERT GUERRA: Robert Guerra.

JULIE HAMMER: Julie Hammer, je ne suis affiliée avec personne.

DANNY MCPHERSON: Monsieur McPherson, VeriSign.

PAUL EBERSMAN: Paul Ebersman, Comcast.

CRISTIAN HESSELMAN: Monsieur Hesselman.

PATRIK FÄLTSTRÖM: Nous avons bien sûr toutes les personnes qui font partie de notre personnel de soutien ou de support qui est là. Bonjour à tous.

Nous allons vous donner donc une mise à jour sur ce que nous faisons à SSAC. Nous allons vous parler du travail qui est en cours. Nous allons parler des grandes étapes à venir. Nous allons vous parler des publications qui ont été émises et, ensuite, nous allons parler avec vous et donc vous demander si vous avez des questions à nous poser. C'est pour ça qu'il est bon d'avoir tous ces experts au panel avec moi pour pouvoir répondre à vos questions.

En ce moment, nous avons 31 membres. Les membres sont nommés par le conseil de l'ICANN et nous consultons avec le conseil sur tout ce qui se rapporte à la sécurité et l'intégrité de systèmes d'allocation d'Internet au niveau des noms et des adresses.

Nous publions donc des rapports et notre portée est liée aux identifiants et aux systèmes donc d'allocations et d'adresses.

Nous avons des experts de tout genre dans tous les domaines. Comme vous le voyez sur la diapositive, nous avons une grande liste. Nous sommes experts en beaucoup de choses. La chose la plus importante dans tout cela, c'est quand nous nommons de

nouveaux membres à SSAC, nous le faisons nous-même. Nous essayons de nous assurer autant que possible que le SSAC en général a donc l'expertise qui est nécessaire pour pouvoir faire des rapports qui soient adéquats.

Jusqu'à maintenant, nous avons publié 91 documents ; nous en avons distribué un cette semaine et ces publications sont divisées entre les rapports, des papiers de consultation et des commentaires. Et entre tous ces documents, vous pouvez trouver les informations qui concernent le SSAC.

Tous les membre de SSAC et beaucoup d'entre vous dans la salle peuvent parler des choses qui ont à voir avec la sécurité. Mais tout ce que nous disons, tout ce que nous exprimons dans ces rapports, correspond à ce que nous faisons et ce que nous disons.

Donc, la charte de la SSAC est liée aux valeurs de base de l'ICANN. Il s'agit d'assurer la sécurité d'Internet et de préserver la stabilité… et la… et la stabilité d'Internet.

Notre rôle principal, c'est de donner des conseils, des avis au conseil de l'ICANN et c'est ce que nous faisons avec nos recommandations. Et notre charte est donc liée à la mission de l'ICANN.

Lorsque nous soumettons des considérations au conseil de l'ICANN, nous soumettons cet avis à… au bureau… au conseil d'administration. Le conseil en prend connaissance et, ensuite, il peut faire une des quatre choses.

Ils peuvent alimenter ce document, cet avis, dans le processus d'élaboration de politiques. Ils peuvent demander au personnel de mettre en œuvre cet avis en passant par un processus de consultation publique. Ils peuvent disséminer l'avis aux parties concernées, ou ils peuvent choisir une solution différente tout en expliquant pourquoi ils ont choisi cette autre solution, autre que celle qu'avait suggéré le SSAC.

Tout cela ne veut pas dire que le conseil doit faire ce que nous voulons. Personne n'a à suivre nos conseils ou nos avis, mais, bien sûr, nous, nous pensons que c'est le meilleur avis du monde et que si vous ne suivez pas notre avis, le ciel va vous tomber dessus.

Mais nous sommes juste un comité consultatif et vous devriez tous lire nos avis et, bien sûr, si vous pensez que notre avis est correct, vous pouvez le suivre.

Le travail qui est en cours en ce moment est lié à l'harmonisation des IDN. Nous suivons le travail de la gestion de l'espace des noms et du risque de délégation des nouveaux TLD. Et nous avons émis une publication qui s'appelle SSAC 90, 91…

SSAC 90 et SSAC 91. C'est donc du travail qui est en cours et nous pensons qu'il y a peut-être encore du travail à faire.

Nous avons des groupes de travail qui travaillent sur l'atelier DNSSEC. D'ailleurs, il y a eu une réunion aujourd'hui et nous avons le comité d'adhésion qui donc évalue les membres SSAC et les membres potentiels qui sont candidats au bureau membre de SSAC.

Nous avons publié les document 85, 86 et 87, qui sont liés à… Pardon. Alors, 85, 86 et 87 qui étaient des réponses au PDP GNSO, donc du groupe de travail et le numéro 89 qui était la réponse aux commentaires de la ccNSO pour le SSAC 84. C'était donc lié aux processus EPSRP de la GNSO. Le numéro 91 qui était lié aux indicateurs de santé et 92 qui est lié aux questions qui ont à faire avec les droits de l'homme. Voilà donc. Ce sont des choses dont on a déjà parlé d'ailleurs.

Donc, si vous regardez les grandes étapes à venir ou qui ont été faites. Nous avons publié le… nous avons… nous espérons publier en 2017. Il y a encore des documents que nous devons livrer avant la fin de l'année. Nous aurons donc l'atelier de travail pour l'ICANN 59. Nous regardons aussi le travail qui va être fait dans le DNS avec les nouveaux gTLD, la nouvelle série de gTLD.

Si vous regardez… nous regardons un peu les détails de ces publications que nous avons émises depuis la dernière réunion de l'ICANN, dans le SSAC 91, nous avons révisé la présentation sur les indicateurs de santé et nous avons fourni une réponse… Nous avons donc émis une réponse et nous avons…

Nous nous sommes rencontrés avec les personnes qui avaient… avec les groupes de l'ICANN et nous avons discuté de cela cette semaine aussi. Nous avons certains problèmes avec le choix de la terminologie. Il y a eu des mises à jour qui ont été faites. Nous avons aussi des problèmes avec le manque de distinction entre la collecte des données et les conclusions qui sont tirées de ces données.

Dans SSAC 90, nous avons une consultation sur la stabilité du DNS. Nous avons donc fait des observations et des recommandations pour mitiger les risques identifiés. Dans le SSAC 88, SSAC 89, nous avons clarifié certains problèmes qui avaient été soulevés durant le SSAC 84 liés aux processus du ccNSO qui sont liés à la réévaluation des évaluations qui avaient échouées durant les allocations de TLD. La ccNSO a émis un rapport sur les processus EPSRP et nous avons quelques problèmes à … Nous avons trouvé quelques problèmes à ce sujet-là.

Donc, il y a des discussions en ce moment entre la ccNSO et le SSAC. Après le 89, nous avons eu plusieurs réunions entre le ccNSO et le SSAC. D'ailleurs, cette semaine, même ce matin, nous nous sommes rencontrés, donc il y a des progrès qui sont faits sur ce sujet.

Voilà donc des exemples de questions qu'on nous pose sans arrêt sur la priorité, comment nous mettons les priorités sur certains de nos travaux. Je vais y passer assez rapidement et, ensuite, je vais demander à mes collègues ou vous dans la salle de poser des questions pendant les 45 minutes qu'il nous reste.

Nous mettons en priorité les nouveaux travaux si vous voulez. Nous choisissons nos projets. Si nous recevons une question du conseil de l'ICANN, dans ce cas-là, nous mettons cela dans notre liste de priorités parce que notre tâche principale est de consulter avec le conseil de l'ICANN.

Nous avons des délais que nous devons respecter et, dans ce cas-là, nous essayons de livrer ce rapport à temps, donc avant la date butoir et je pense que nous avons réussi à le faire, et à soumettre nos commentaires, nos suggestions durant les délais prévus.

Nous posons aussi des questions et nous donnons des recommandations sur la base des problèmes qui nous sont envoyés par d'autres unités constitutives de l'ICANN. Je pense

que, l'année dernière, nous n'avons reçu que… Nous n'avons reçu aucune demande. Nous aimerions en avoir, car quand nous faisons nos propres enquêtes sur des problèmes que nous trouvons nous-mêmes… Donc, nous choisissons des éléments, nos éléments de travail ou nos projets nous-mêmes.

Nous recevons aussi des questions… comment est-ce que… sur le fait que nous suivons les réponses. Comment est-ce que nous suivons les réponses du conseil d'administration ? Le conseil d'administration doit agir sur notre avis, sur l'avis que nous émettons.

Et nous avons fait un suivi là-dessus. Nous savons que, souvent, entre le conseil d'administration et nous, cela ne se passe pas forcément toujours très bien. Donc le conseil d'administration développe quelque chose qui s'appelle, disons, un contrôle.

C'est un projet de contrôle pour voir comment cet avis est suivi et ce programme, ce système, n'est pas encore prêt. Mais les mécanismes derrière ce processus sont prêts. Donc, nous SSAC, comme tous les autres groupes qui doivent émettre des rapports, nous savons où en sont les avis dans le processus de l'ICANN. Donc maintenant, nous savons que le suivi est automatique.

La prochaine question, c'est comment est-ce que SSAC informe la communauté sur son travail ? Donc, on le fait comme on le fait

aujourd'hui. On vous explique ce qu'on fait, ce qui est courant, mais nous le faisons aussi à travers la publication d'un rapport. Nous avons aussi la page web où nous publions tous nos documents, nos statistiques et nous avons une page [inaudible] sur les pages ICANN. La page web que nous avons avec nos documents est donc la page la plus intéressante pour chacun d'entre vous. D'ailleurs, pour nous aussi, qui sommes intéressés sur le SSAC.

Les personnes qui viennent voir nos documents sur la page, sur notre page, passent en moyenne trois minutes à lire nos documents, à lire ces mêmes documents.

Nous avons aussi une page Facebook. Nous essayons d'y mettre quelques vidéos pour… que nous publions… que nous… avec l'équipe de l'ICANN qui nous aide dans ce cas-là. Nous avons des réunions. Nous essayons de faire participer nos membres SSAC à des événements au niveau régional. Donc si vous avez besoin d'un de nos représentants qui vienne faire une présentation de l'information ou vous informer sur ce que nous faisons maintenant, vous pouvez faire cette demande.

Nous sommes des personnes qui se préoccupent de la sécurité, pas du commerce. Donc je voudrais remercier Duncan pour nous aider à comprendre comment nous pouvons ainsi communiquer avec le reste de la communauté.

La dernière question a à voir avec… Donc quand on parle du suivi, que peut faire la communauté vis-à-vis de notre avis au conseil d'administration ? C'est ce que je vous ai dit tout à l'heure. Ce n'est pas encore très facile de faire notre suivi. Nous avons un peu d'aide de la part du personnel de l'ICANN, mais c'est à peu près où nous en sommes en ce moment.

Voyons maintenant. Je vous passe la parole. Voilà avec les questions que j'ai sur l'écran. Maintenant, je voudrais vous donner la parole pour que vous puissiez émettre vos questions. Posez des questions, on verra bien ce qu'on va vous répondre.

Je vais tout d'abord demander dans la salle de demander à mes collègues s'ils ont… si mes collègues membres du SSAC ont des choses à dire.

PERSONNE NON IDENTIFIÉE: Oui. Nous avons vu durant les six à neuf derniers mois qu'il y a eu… que les attaques, vous savez, sont devenues… ont pris des proportions incroyables. Nous savons qu'Internet est un milieu hostile. Ce n'est pas l'Internet dont nous avons rêvé. C'est devenu un monde très, très dangereux.

Qu'allons-nous faire à ce sujet ?

PATRIK FÄLTSTRÖM: Si vous êtes dans l'audience, vous pouvez venir au micro.

Alors, lorsqu'il s'agit… Attendez, quelqu'un veut prendre la parole. Très bien.

JONATHAN MAKOWSKI: Monsieur Makowski. Merci pour le travail que vous faites pour la communauté. Deux ou trois choses dont je voulais parler pour avoir un peu de suivi.

Quand il s'agit des carences DNSSEC et des directives qu'il devrait y avoir de la part du comité par rapport à ces carences que ce soit… Pour tout ce qu'il s'agit de ces problèmes. Je sais que le gouvernement suit ce travail là-dessus en ce moment, mais je ne sais pas si vous en discutez au sein de votre groupe ou si c'est un sujet d'importance pour vous ou pour votre communauté.

J'ai d'autres questions, mais, pour l'instant, je vais en rester là.

PATRIK FÄLTSTRÖM: Je ne sais pas si quelqu'un est au courant de cette chose là ou travaille sur ce sujet ?

ROD RASMUSSEN: Alors, c'était… Donc, ce sujet de [inaudible] de trou, de carence était un sujet qui était sur la table, mais je ne savais pas que c'était encore courant.

Et pour ceux qui sont dans la salle, ce qu'on appelle le sinkhole DNSSEC, donc est celui-ci. Si votre nom de domaine est utilisé pour quelque chose qui… pour du malware ou quelque chose qui est hors de votre contrôle.

Donc, ce qui se passe dans ce cas-là, si vous êtes, vous faites partie des forces de l'ordre ou si vous êtes d'une compagnie de sécurité, et bien ces domaines seront retirés par l'opérateur de registre et remis en… dans… remis donc pour pouvoir être réutilisés. Cela dépend si on a des arrangements qui sont fait avec les bureaux d'enregistrement.

Donc, tous les ordinateurs qui sont infectés continuent à atteindre le même serveur et donc on peut voir que les ordinateurs qui sont affectés… les ISP sont au courant, reçoivent des avis et peuvent ainsi utiliser toutes ces données pour faire des recherches.

Certaines compagnies ont… Certaines entreprises ont construit leurs affaires avec ces données. Donc, c'est pour ça que cette question d'éthique, de déontologie, est arrivée sur la table. Il y avait des entreprises de sécurité il y a quelques années qui volaient ces sinkholes, ce qu'on appelle ces sinkholes, ces carences d'autres entreprises.

Donc, le thème reste important et un autre exemple d'ailleurs de ce qu'on appelle un sinkhole. C'est l'algorithme de génération

des domaines, DGA. Encore un acronyme pour vous d'ailleurs. Bon, avec le DGA, ce qui se passait à l'époque – d'ailleurs l'ICANN s'en est occupé il y a quelques années – donc ce qui se passait à ce niveau-là, c'est que l'algorithme avait une liste de plusieurs douzaines, même des milliers de noms de domaine, donc des domaines qui n'étaient pas forcément enregistrés. Donc, c'était des bonnes données pour les chercheurs dans le domaine de la sécurité, parce qu'ils pouvaient ainsi finir ou continuer leur enquête.

Donc, les politiques à ce sujet sont un petit peu souples. Il y a un effort qui a été fait. On en a parlé durant les réunions passées de l'ICANN et il y a des groupes qui essaient de normaliser ces opérations appelées sinkhole. Donc il y a des personnes qui travaillent pour des entreprises de sécurité qui utilisent ces nouveaux systèmes pour créer un espace qui s'appelle l'espace toxique des domaines toxiques. Mais, encore une fois, ce sont des projets qui viennent juste de commencer.

Et il y avait eu donc un scandale qui avait commencé en 2008, je crois, et ces domaines ont été gérés par ce nouveau système d'ailleurs. Donc, depuis toutes les personnes responsables ont été arrêtées. Nous aimerions donc continuer à parler de ce sujet.

DANNY MCPHERSON: Je voudrais continuer avec ce qu'a dit Rod. Nous avons des activités opérationnelles comme les retraits, ce qu'on appelle retrait Avalanche, et nous avons d'autres activités qui ont des impacts sur les consommateurs, tout ce qui est cybercriminalité, toutes sortes d'activités qu'on puisse imaginer.

Donc, du moment que le nom de domaine est utilisé pour que les gens, n'importe qui puisse naviguer sur Internet, nous, on doit faire tout ce qu'on peut dans cette communauté pour mettre en place des systèmes de protection. Donc, une nouvelle façon de voir les choses maintenant, c'est de continuer à travailler là-dessus et d'essayer d'être plus efficace. Il y a aussi un groupe de sécurité publique qui travaille sur ces systèmes de protection pour le consommateur d'ailleurs.

Aussi, il y a plusieurs documents qui ont été écrits sur le bon fonctionnement d'Internet et qui expliquent les espaces dans l'Internet qui ne sont pas forcément très bien codifiés. Et, bien sûr, il y a une certaine coopération avec les forces de l'ordre qui est importante. Il faut trouver un moyen d'avoir un impact au niveau de la sécurité à plutôt long terme.

Il faut continuer à protéger les infrastructures et tout ce qui concerne les entreprises sur Internet. Toutes ces choses qui sont utilisées maintenant et qui ne seront plus utilisables dans l'avenir.

Au niveau opérationnel, il y a tellement de choses qui sont importantes. On essaie de travailler en collaboration avec l'ICANN et du côté opérationnel, du côté sécurité et des opérateurs de registre, on essaie d'aider pour combattre cette menace. Donc il n'y a rien que le SSAC peut faire ou peut dire qui puisse vraiment avoir, ou du moins on essaierait d'avoir un petit peu plus d'impact. Puisque tous ces problèmes deviennent tellement, tellement divers et tellement vastes.

PATRIK FÄLTSTRÖM: Le membre numéro un de SSAC qui travaille avec les opérateurs de registre ou le registre de fallback dont il parlait n'est pas là. Sinon on pourrait parler de ce sujet beaucoup plus.

DAN YORK: Je n'ai pas de question, mais je voulais vous dire que quand vous avez mentionné les activités, que vous avez parlé de l'atelier du DNSSEC… Donc, je peux vous dire que l'atelier vient juste de se terminer. Il y avait à peu près une centaine de personnes qui sont venues participer. Il y avait de très bonnes présentations. Je vous encourage tous à aller en prendre connaissance.

Nous avions un panel qui comprenait .DE, .AT, .DK, .CZ, qui étaient présents.

Nous avons eu aussi une séance avec les ISP et Paul Ebersman était là. Il représentait Comcast. Il nous a expliqué comment les ISP se préparait pour avant le KSK.

Donc, nous avons parlé de la sécurité des courriels et ce qui se passe au sein de SSAC, c'est que le support qu'ils peuvent offrir pour que tous ces projets soient mis à jour.

Pour tous ceux qui sont intéressés par les statistiques, il y avait une personne de SURFnet qui a fait une présentation sur le déploiement du ECDSA et là il y avait beaucoup de statistiques intéressantes qui pourraient être importantes pour beaucoup de personnes qui sont là.

Roland est aussi intéressé dans la coordination d'un effort vers la… qui porterait sur les… la façon dont on pourrait mesurer les DNS. Le 11 juillet, on sait très bien que la nouvelle clé va être introduite et donc on en a parlé. Je voulais donc en attendant remercier le SSAC pour leur soutien à cette session de… à cette séance du DNSSEC. C'était une bonne séance aujourd'hui.

PATRIK FÄLTSTRÖM: Merci beaucoup. Vous [inaudible] qu'on a absolument aucune intention de mettre fin à cette coopération. Continuons à faire les choses bien ensemble.

Personne suivante.

MARIA HALL: Bonjour, [inaudible]. Je suis membre du bureau exécutif RIPE NCC et également présidente du chapitre ISOC suédois. Peut-être que vous pourriez développer un peu ce que vous avez dit monsieur. Parce que… Excusez-moi, j'ai oublié votre nom.

ROD RASMUSSEN: Rod Rasmussen.

MARIA HALL: Rod, pourriez-vous développer ou d'autres de vos collègues ce que vous avez dit par rapport au développement de l'Internet des choses et, dans quelle mesure, c'est lié à ce que vous disiez auparavant. Bien entendu qu'il y a un lien, mais j'aimerais que vous approfondissiez un petit peu ce lien, que vous le développiez. Et en tant que présidente du chapitre ISOC suédois, nous avons eu une séance la semaine dernière avec une assemblée, et la réunion du conseil d'administration. Et on parlait d'une règlementation, d'une législation, on ne sait pas pour que tous les fournisseurs puissent… Parce que tout est connecté, depuis nos brosses à dents jusqu'à nos ordinateurs portables. Tout est connecté.

PATRIK FÄLTSTRÖM: Alors, une des choses sur laquelle on a travaillé au SSAC, mais qui n'apparait pas dans le rapport – parce qu'on ne sait pas

encore à qui donner cette recommandation, c'est que l'un des plus grands problèmes de l'Internet des choses, c'est que les gens les achètent, les collectent et, ensuite, ils ne les touchent pas, ces choses-là. Les gens n'actualisent pas non plus ou n'améliorent pas leur logiciel, leur programme, et il y a beaucoup trop de choses que vous ne pouvez pas non plus actualiser.

Donc ça, c'est un autre problème. Concernant la législation, si on force les gens, c'est comme si on disait aux criminels qu'ils ne peuvent pas rentrer voler dans des maisons, cambrioler des maisons. Ça ne sert un petit peu à rien. Je ne sais pas si l'un de mes collègues veut ajouter quelque chose ? Danny ?

DANNY MCPHERSON: Oui, je dirais simplement qu'il y a un certain nombre d'endroits où on parle de ça, mais il faudrait en parler peut-être lors du forum public.

Les opérateurs de registre qui participent dans différents endroits de l'écosystème, que ce soit au niveau des TLD, des noms de domaine de second niveau qui reçoivent toute une série d'attaques peuvent en parler. Mais, bien entendu, nous, on prend cette question extrêmement au sérieux, tout ce qui concerne la vulnérabilité de l'infrastructure et l'intégrité de cette infrastructure.

Et on essaie d'établir un réseau de confiance et lorsqu'il y a ce genre d'attaques, c'est réellement problématique parce qu'il faut que la communauté ICANN renforce cette sécurité. Ça, c'est une partie du problème.

L'autre partie, c'est que lorsqu'on en revient au document SSAC 04 anti-spoofing, on voit qu'il y a tout un problème par rapport aux activités des DDoS.

Et certains des codes d'attaque qui sont en particulier utilisés, donc ça c'est l'autre partie du problème.

Ensuite, il y a un plus grand problème, plus général en termes d'opération, et je pense que beaucoup des gens qui participent à cette communauté ont une influence, ont un mot à dire là-dessus. Mais il y a un cadre OIT entre la matière et le FTC, le NTIA et d'autres dans ce domaine qui parlent de bonnes pratiques.

Mais s'il y a ce genre de problème qui va se poser de plus en plus à l'avenir, essayons de travailler tous ensemble pour garantir la sécurité, l'interopérabilité, et essayer de se protéger de ce genre d'attaque et d'activité en particulier, surtout lorsqu'elle porte atteinte à l'espace des noms.

Donc, il faut renforcer notre capacité à répondre aux attaques des DDoS et d'autres, et sachez qu'on les prend très, très au sérieux.

GEOFF HUSTON: Oui. Il y a deux aspects à cela. D'abord, l'industrie des logiciels qui est un échec total au niveau commercial. Il y a un marché pour les choses peu chères sur l'Internet des choses.

Et nous avons une chaîne d'approvisionnement qui est mondial et donc cette chaîne est éphémère et on est pris dans une situation où le réseau zombie recrutait des gens sur Internet, un protocole que personne n'utilisait pendant 30 ans, sauf peut-être pour des caméras vidéo.

Et ça, c'est extrêmement mauvais. Il n'y a pas de mécanismes concernant cette chaîne d'approvisionnement. Ce qu'on a observé toutefois, c'est qu'il n'y a que deux protocoles qui fonctionnent pour ce genre de choses : HTTPS et DNS. Et c'est là que le DNS a un point de vulnérabilité.

Dans le cas d'un réseau zombie, le point de commande de contrôle, c'est le DNS. Donc à chaque qu'on [inaudible] des millions d'outils, le DNS est toujours là.

Et c'est là que le travail pour savoir si le DNS peut signaler s'il y a ce genre de choses qui se produisent et qui font interférence, ça, ça rend les gens totalement désespérés.

Parce qu'il y a sept milliards d'outils qui sont disponibles sur Internet et que pouvons-nous faire ? On peut juste espérer faire

quelque chose de productif par rapport au DNS pour contrôler cette chaîne d'approvisionnement. On essaye. Est-ce qu'on y arrive ? Pour l'instant, non, mais on essaye.

PATRIK FÄLTSTRÖM: Rod.

ROD RASMUSSEN: Alors, pour ne pas être aussi pessimiste que mon prédécesseur, je dirais qu'il faut parler du problème fondamental ici et Geoff en a bien parlé d'ailleurs. Lorsque vous pensez à l'Internet des choses, on s'aperçoit qu'il y a plus de choses sur Internet qu'il n'y avait avant, des choses qui sont plus grandes aussi. Donc, on a un certain nombre de problèmes à régler.

D'abord, c'est l'échelle. Il faut voir l'ampleur d'Internet de maintenant à dans dix ans. Ensuite, la mauvaise utilisation de cette infrastructure et le problème vis-à-vis de ces outils, c'est justement les fabricants qui ne sont pas des entreprises de logiciels. Donc il y a des bibliothéques, etc., qui incluent des choses qui ne devraient pas faire partie de ce paquet technologique.

Et ça fait maintenant combien d'années qu'on essaie de convaincre Microsoft d'adopter un code de conduite et ils font un bon travail à ce niveau-là.

Il y a beaucoup de normalisation et de débats par rapport à la normalisation, mais il faut sécuriser les choses avant de les mettre sur Internet. Donc, il y a des analogies qu'on peut faire par rapport à ce qui se produit dans la vie réelle. On ne va pas résoudre le problème au niveau des outils et il y a une échelle incroyable de ce problème. Donc ça, c'est très difficile, mais il y a des points d'accès qu'on peut utiliser. On peut faire des choses par rapport à l'infrastructure ou on peut chercher des choses qui sont connectées à Internet d'une manière dont elles ne devraient pas l'être.

Et très peu de personnes font cette chose-là actuellement. Donc, il y a des petites choses qu'on peut faire en tant qu'opérateurs d'infrastructure qui contrôle le réseau, etc.

Donc, j'espère qu'on peut en tout cas essayer d'améliorer les choses.

WARREN KUMARI: Warren, moi-même, c'est-à-dire… j'essaie de décider si j'interviens ou pas. Alors, on parle de l'Internet des choses, ce qui veut dire un peu tout et rien.

Comme beaucoup de gens l'ont dit, c'est beaucoup d'outils, beaucoup d'outils qui sont fabriqués de manière aussi peu onéreuse que possible.

Donc, fabriqués par des petites entreprises qui n'ont pas le logiciel comme principale technologie ou compétence et qui réunissent quelques trucs ensemble et qui espèrent que ça va voler.

Donc les PCP, ce genre de document, je ne pense pas que ça nous amène à grand-chose. Elles n'essaient pas, ces entreprises, de suivre des bonnes pratiques, mais simplement de vendre des choses.

Donc, essayer d'avoir un contrôle quel qu'il soit sur la chaîne d'approvisionnement ou essayer de voir quel type d'outil est en train de parler à quel autre ou est connecté à quel, ça, ça ne va pas nous aider.

Parce que quand on parle de l'Internet des choses, c'est très difficile de voir quel est le problème parce qu'on voit qu'il y a beaucoup d'aspects. C'est difficile de voir pourquoi ces entreprises font ce qu'elles font.

Moi, je pense que ce qui marcherait le mieux, ce serait d'améliorer certains des CPE et que les gens ou les fabricants en général ne soient plus propriétaires de leur propre code en termes de CPE. Ils utilisent un logiciel comme Tomato ou autre.

PERSONNE NON IDENTIFIÉE: Qu'est-ce que veut dire CPE ?

WARREN KUMANI: C'est un équipement pour client, un pare-feu si vous voulez. Donc, en général, les gens écrivent leur propre code source et ils modifient la page principale.

Donc, si on pouvait créer un cadre ou un paquet d'outils qui permettrait de faire en sorte que vous puissiez télécharger un logiciel, vous sélectionnez les modules que vous voulez, vous mettez votre logo et donc vous ressemblez à cela. Alors ça serait moins cher que les gens qui fabriquent de zéro.

Donc, on pourrait élaborer des cadres que les fabricants pourraient utiliser et on les encouragerait à l'utiliser, parce que, quand ces fabricants fabriquent de zéro, ça revient beaucoup plus cher.

PERSONNE NON IDENTIFIÉE: J'aimerais élargir un petit peu le débat, parce qu'il y a 25 ans j'ai fondé une entreprise de sécurité. Or, aujourd'hui, on a l'expérience et on sait que certains outils sont dépassés, parce qu'il y a la question de la conformité. Vous ne pouvez pas patched les… Vous ne pouvez pas patched ce genre d'outil.

Et deuxièmement, vous avez parlé de la sécurité de [inaudible], mais nos clients, ce qu'ils veulent, c'est avoir une vision là-dessus. Donc nous avons des pare-feu NG qui font voler en éclat ces attaques de l'homme du milieu et il y a des choses qui sont

vertes, mais qui ne sont pas vertes parce qu'elles sont interceptées, etc.

PATRIK FÄLTSTRÖM: Concernant votre premier commentaire sur la conformité, comme vous le disiez, il a d'autres aspects qui entrent en jeu. C'est l'une des raisons pour laquelle en tant que président du SSAC, nous au SSAC, nous n'avons pas trouvé réellement où est le problème. Comment limiter le problème ?

C'est difficile de se concentrer sur quelque chose en particulier et c'est difficile aussi d'essayer de donner une recommandation qui permettrait d'améliorer les choses, parce qu'écrire des documents sur les problèmes liés à l'Internet des choses, comme on le voit ici, c'est très difficile.

Dans cette salle, on pourrait écrire 60 pages de documents là-dessus, mais mesurer l'effet ça c'est vraiment difficile.

Concernant la deuxième partie de votre commentaire, les connections TLS, nous à SSAC, nous avons élaboré un certain nombre de recommandations par rapport à l'utilisation de certificats de manière plus efficace, en particulier le mécanisme CA des certificats qu'on utilise actuellement.

Et on a répondu au ITU-D qui nous a envoyé une liaison en pensant que ce serait une bonne chose de lancer des nouveaux

CA dans le monde entier. Donc il y a un nombre très élevé de CA et notre réponse, ça a été non, il faut agir de la manière inverse.

Donc, je pense que le SSAC pense que le TLS et ce genre de mécanismes devraient continuer d'être utilisés. Par exemple, continuer d'utiliser DANE et d'autres technologies de ce genre et on l'a dit à plusieurs reprises.

Parce que quand on a une menace, c'est une menace commune vis-à-vis de ce genre de certificat.

Est-ce que d'autres membres souhaitent intervenir ? Personne dans la salle ?

PERSONNE NON IDENTIFIÉE: Bonjour. Je viens de l'Université d'Oxford. Moi, ce qui m'intéresse, c'est de savoir quel est votre intérêt dans les recherches par rapport à la sécurité ? Qu'est-ce que vous pensez qu'on devrait étudier par rapport à la sécurité ?

GEOFF HUSTON: Oui. Moi aussi, je fais beaucoup de recherches et je dois avouer que mon dada, c'est un petit peu de comprendre ce qui se passe à l'intérieur, mais aussi à l'extérieur.

C'est toujours facile de mesurer quelque chose à l'intérieur, mais, ensuite, il faut le comparer à ce qui se passe à l'extérieur.

Parce qu'il y a ce que vous faites, vous, et ce que font les 3 milliards d'autres utilisateurs de l'Internet.

Il y a un cas de réussite, notamment les programmes de mesure pour voir la pénétration de l'IPv6 dans le temps et faire de l'introspection également dans le système des noms de domaine et voir combien des utilisateurs de l'Internet dans le monde ne vont pas sur un nom de domaine s'il n'est pas bien signé ou validé par le DNSSEC.

Et ça, c'est très important, parce qu'ils peuvent faire la différence entre ce qui est une bonne validation et non. Et ça, c'est incroyable. On a un nombre de validations du DNSSEC énorme.

Je crois que mon propre pays, l'Australie, ne [inaudible]. Donc ça, on peut le faire pays par pays et fournisseur par fournisseur. Et ça, il faut voir ce qui se passe à l'intérieur comme à l'extérieur, parce qu'Internet c'est nous tous, et c'est aussi les gens qui sont au bord des limites, des frontières.

WARREN KUMARI: Il faut voir aussi comment les choses fonctionnent dans les différents pays, mieux comprendre les choses que vous pouvez atteindre et les choses que vous ne pouvez pas atteindre, en raison de la censure et d'autres…

Pourquoi est-ce que je ne peux pas atteindre un… Je ne peux pas avoir accès à un site spécifique dans un pays ou dans un autre.

DANNY MCPHERSON: Oui. Par rapport à ce que disent Geoff et Warren, effectivement, c'est un travail très intéressant par rapport à toutes les études qui sont en cours.

Je vous les cite rapidement d'ailleurs, mais étant donné qu'on a plus de 300 ccTLD et une grande majorité d'entre eux n'ont pas de nom enregistré pour les ccTLD.

Donc, « de quoi est-ce que je dépends pour les opérations sur l'espace des noms de domaine dans mon pays ? » C'est ce genre de question.

Ou comprendre l'infrastructure multi-niveaux et d'autres exemples où une personne peut pirater une centaine d'entreprises.

Je pense que les choses vont empirer à mesure que l'infrastructure va augmenter. Donc, il y a des implications en termes de sécurité, pas seulement pour le DNS, mais aussi pour l'infrastructure d'Internet au sens plus large, également les intérêts nationaux de la sécurité du pays. Ça aussi, ça va entrer

en jeu. Et voir dans quelle mesure l'infrastructure et l'interdépendance vis-à-vis de la sécurité nationale sont liées.

CRISTIAN HESSELMAN: D'abord, il faut que les utilisateurs finaux puissent avoir un plus grand contrôle sur la sécurité et l'aspect confidentialité des services qu'ils utilisent chez eux. Par exemple, et ça c'est lié à la conversation IT qu'on vient d'avoir, parce qu'une hypothèse, ça pourrait être s'ils sont conscients des vulnérabilités de sécurité, ils peuvent éteindre cet outil, le déconnecter du réseau pour se protéger eux-mêmes et les opérateurs dans l'infrastructure DNS.

Autre question aussi, comment les différents opérateurs DNS et parties pourraient analyser de manière conjointe les données et partager ces données entre eux pour ce qui concerne la sécurité.

PATRIK FÄLTSTRÖM: Oui. Personne suivante.

WES HARDAKER: Par rapport à la discussion que vous avez-vous et que nous avons, nous, on a tendance à classer les choses et les pays. C'est un exemple.

Une étude très intéressante du SSAC, c'est de voir combien de catégories mesurables existe-t-il. Ça, on n'y pense pas. Quel est

le pourcentage de validations DNSSEC qu'il y aurait pour les ISP ?

Et on sait que les choses ne fonctionnent pas comme ça. Qu'est-ce qu'on pourrait avoir à notre disposition ?

Je ne sais pas si on pourrait y réfléchir ensemble. Je ne sais pas, mais j'ai l'impression qu'il y a beaucoup d'autres paramètres ou mesures qu'on pourrait utiliser pour comparer les pays les uns aux autres.

PATRIK FÄLTSTRÖM: Geoff.

GEOFF HUSTON: Oui. Lorsque vous regardez les documents qui existent actuellement, vous vous apercevrez que, et c'est ce qu'on a publié dans notre rapport, c'est que si vous publiez des données par pays… Alors, lorsque vous publiez ce qui concerne les nombres autonomes, ça se complique.

Parce que vous n'allez pas forcément dire ce que le lecteur veut lire.

NICK SHOREY: Bonjour. Nick Shorey au micro. Je représente le gouvernement britannique. Récemment, nous avons commencé à nous pencher sur l'Internet des choses et la sécurité par défaut. Pour

revenir sur ce que vous disiez de la faisabilité, ce qui me préoccupe toujours, c'est de voir que vous avez…

Comme vous l'avez dit, toutes ces entreprises qui ne sont pas du tout spécialisées dans la technologie informatique et qui se mettent à fabriquer des outils informatiques parce que c'est à la mode. Moi, ce qui me préoccupe, c'est le nombre croissant d'outils qui sont obsolètes et qui sont connectés.

Donc, j'attends avec impatience vos conseils, avis pour voir comment régler ces problèmes, ces problèmes d'outils obsolètes qui sont connectés. Est-ce que vous pourriez m'indiquez un document ou une recherche que je pourrais partager avec mon gouvernement pour approfondir ce sujet ?

WARREN KUMARI: Veuillez m'excuser, mais je crois que je ne vais pas vous donner de bonnes nouvelles. Récemment, je cherchais un point d'accès pour ma maison et j'ai commencé à essayer d'en trouver un pas cher. Donc, j'ai été sur Alibaba, un site très connu, et j'ai trouvé près de 700 entreprises qui fabriquent exactement le même outil.

Donc, vous en étudiez une centaine, vous les sélectionnez et vous en trouvez une autre centaine. Donc, le fait de leur fournir des actualisations, ça n'empêche pas que de nouvelles entreprises commencent à faire la même chose.

Donc une option, ce serait, et je crois qu'elle a été proposée il y a quelques années, c'est que vous achetez un routeur pour votre maison, vous l'utilisez pendant deux ans et ensuite vous le changez.

Et lorsque les choses sont moins chères, alors elles ne marchent plus et il faut les changer.

ROD RASMUSSEN: Alors, en fait, je pense que les choses sont bien pires. Parce que lorsque vous demandez aux gens qui vendent des smart car… On se demande est-ce que vous avez un manuel pour tous les outils électroniques de votre maison ?

Et la bonne nouvelle, c'est ce qu'a dit Danny avant. Parce qu'il y a toutes ces informations sur la manière de faire face à ça dans le monde entier, et il y a une manière de traiter toutes ces questions. Ce n'est pas une chose nouvelle d'ailleurs. Il y a des gens qui ont travaillé pour voir voilà quelles sont les idées règlementaires pour tel secteur d'activité, etc.

Et parfois, ça marche. Vous voyez qu'au SSAC on n'est pas tous d'accord, mais bon, vous le voyez, il y a des efforts sérieux qui vont dans ce sens et je peux continuer à en parler avec vous d'ailleurs après.

ROBERT GUERRA : Oui. Pour revenir sur ce qu'a dit Warren, Ondrej, qui travaille aussi au SSAC, nous a parlé d'une source ouverte pour actualiser les routeurs. Donc, c'est une initiative très intéressante. Peut-être qu'on pourrait partager ce genre d'initiative.

Il y en a d'autres d'ailleurs, et voilà ce que je voulais vous transmettre.

PATRIK FÄLTSTRÖM : Oui. Une autre question.

JAD EL CHAM: Bonjour. Jad El Cham. Je suis boursier. C'est ma première conférence ICANN. D'abord, merci de vos présentations. J'ai une question que je pose depuis trois jours maintenant et je n'ai eu aucune réponse jusqu'à présent.

On continue de nous parler de l'Internet des choses, de DDoS, etc. Mais on semble oublier que les nouvelles formes d'attaque DDoS se concentrent surtout sur deux protocoles, DNS et NTP, et on utilise ces serveurs comme réflecteurs.

Donc maintenant, on entend beaucoup parler de DDoS et de DDoS réflectif. Je ne sais pas votre sentiment, mais nous, c'est ce qu'on voit chez nous, et nous déployons des outils de sécurité pour nos clients.

Donc, ma question est la suivante : le DNSSEC traite beaucoup des vides qui existent par rapport au DNS, mais en termes de sensibilisation par rapport aux lacunes du DNS comme l'utilisation des réflecteurs.

Je sais qu'une des réponses qu'on m'a données, c'est qu'il y a un groupe de travail, l'IETF, qui travaille là-dessus, mais j'aimerais savoir aussi si l'ICANN participe à ce genre d'effort.

PATRIK FÄLTSTRÖM: L'ICANN, à l'instar de beaucoup d'organisations, opère certaines infrastructures. Google s'occupe d'autres infrastructures et, à l'IETF et dans d'autres parties de la communauté, on essaie aussi de travailler pour obtenir les meilleures pratiques, voir comment améliorer ces protocoles, voir quelles sont les faiblesses et quels sont les protocoles les plus populaires pour essayer de parer à ces attaques.

Personnellement, j'ai vu beaucoup de changements par rapport aux attaques utilisées, mais d'une manière générale, on peut dire qu'on a utilisé des adresses IP avec usurpation d'identité et parfois non.

Certains des réseaux zombie sont tellement vastes et tellement difficiles à trouver que… Par exemple, en Suède, on voit que les attaques ne sont pas du tout liées au NTP.

Ce sont des attaques qui utilisent ces protocoles simplement parce qu'il y a une simplification et il faut configurer votre serveur ITP, et certains des routeurs de contrôle ne sont pas utilisés.

Donc, il y a toute une série de choses qui peuvent se produire. L'ICANN est l'organisation qui opère ce genre de chose, travaille sur le processus de développement de politiques et, à ce niveau-là, au niveau du processus de développement de politiques, il y a un travail du côté des parties contractantes et non contractantes où ce genre de choses sont prises en considération lorsqu'on regarde les différentes conditions du côté des parties contractantes, des non contractantes, des meilleures pratiques et pour toutes les unités constitutives de l'ICANN.

Du côté opérationnel, je pense que, nous qui participons à l'ICANN, à l'écosystème de la communauté ICANN, on participe aussi aux forums où ce genre de problème opérationnel est débattu. Est-ce que quelqu'un d'autre souhaite ajouter quelque chose ?

WARREN KUMARI: Donc, quand on parle des attaques qu'on appelle réflexion et l'usurpation des adresses, il y a un document, document 38, qui dit que vous ne devriez pas laisser passer les personnes qui ne

font pas partie de tel ou tel réseau. Il y a un document de SSAC qui dit la même chose. Il n'y a pas beaucoup de choses que l'ICANN puisse faire à ce sujet, mais il y a quelqu'un qui gère le programme MANRS. Est-ce que c'est ISOC ?

Oui. Je pense qu'ISOC a un programme qui s'appelle MANRS, qui gère donc les… qui gère les manières, disons entre guillemets, des réseaux.

Donc, l'ICANN ne peut pas vraiment faire grand-chose à ce sujet. Il ne peut pas donc punir les ISP d'une manière ou d'une autre, à moins que les ASO nous disent qu'ils ne peuvent pas nous donner les informations des ISP qui ne font pas de protection, qui n'opèrent pas de protection au niveau de… contre l'usurpation.

PATRIK FÄLTSTRÖM: Oui. Il est 16 h 15, donc nous en avons terminé. Merci d'être venus. Nous savons maintenant que 15 h 15 le mercredi est mieux pour nous. C'est plus populaire que lorsque nous faisons notre réunion à 8 h 15 le matin, le jeudi. Merci.

[FIN DE LA TRANSCRIPTION]