COPENHAGUE - Session intercommunautaire : Vers une atténuation efficace de l'utilisation malveillante du DNS : prévention, atténuation et réponse
Lundi 13 mars 2017 – 13h45 à 15h00 CET
ICANN58 | Copenhague, Danemark

CATHRIN BAUER-BULST: Bonjour à tous, nous allons commencer notre séance dans quelques minutes, mais entre-temps, je vous prie de bien vouloir vous approcher. C'est une séance qui est consacrée à vous. Donc je vous invite à vous rapprocher de la table pour pouvoir entamer des discussions. Merci beaucoup.

Bien. Bonjour à tout le monde, soyez les bienvenus dans cette séance pour l'atténuation des risques de l'usage malveillant du DNS.

Je m'appelle Cathrin, je suis là avec le groupe de travail qui va vous présenter le thème.

BOBBY FLAIM: Je m'appelle Bobby, je fais partie du FBI, je fais partie du groupe de sécurité publique tel que Cathrin le fait.

CATHRIN BAUER-BULST: Pourquoi sommes-nous ici ? Lorsque vous avons été à Hyderabad, vous devez vous rappeler que nous avons fait un exercice concernant l'atténuation des risques pour l'usage malveillant du DNS.

Aujourd'hui, nous allons vous donner davantage de précisions sur l'atténuation des risques dus à l'usage malveillant qui soit plus efficace.

Nous en avons parlé très souvent, mais cela est beaucoup plus important encore depuis la transition de l'IANA. Nous avons toujours parlé donc du rôle que jouent les parties privées dans cet écosystème. Nous savons de façon générale que ces parties privées n'appliquent aucune loi. Mais comme l'ICANN joue un rôle de plus en plus important dans cette communauté, au sein de cette communauté, il y a donc un contrat entre deux parties. Et nous, par exemple, nous avons un RAA de 2013, ainsi que d'autres contrats où l'on inclut non seulement l'intérêt des deux parties contractantes, mais des tierces parties qui ne font pas partie justement du contrat.

Alors comment faisons-nous pour relever ce défi ? Que faisons-nous en dehors du contrat ? Parce que l'une des parties et l'une des clauses du contrat imposent de garantir la transparence et la sécurité de ce que nous faisons ; le GAC s'intéresse à ce thème, et c'est pourquoi il parraine cette séance.

Bobby va nous présenter davantage de contexte par rapport à la participation du GAC dans ce thème.

BOBBY FLAIM: Bon ce groupe, avec le soutien du GAC, a été créé par suite d'un avis du GAC sur l'atténuation et le DNS et la conformité contractuelle. Donc le GAC et l'ICANN travaillent ensemble en matière de conformité contractuelle. Ils ont fait des recherches indépendantes sur ce que l'on fait en ce moment.

Et nous nous sommes centrés sur trois domaines. Le premier concernant l'avis du GAC concernait le RAA de 2013 ou l'accord, le contrat d'enregistrement du bureau d'enregistrement, et certains points qui se rapportent à des dispositions du RAA concernant le WHOIS, l'accréditation de précision, etc.

Nous avons, en fait, une validation croisée des adresses dans les spécifications du WHOIS, et d'autres points que nous voulons vérifier en ce qui concerne l'avis du GAC et les dispositions du RAA 2013 concernent les activités que nous pouvons mener à bien suivant le contrat pour que la conformité contractuelle soit beaucoup plus forte, et que l'on puisse vérifier tous les problèmes qui pourraient se présenter par un usage malveillant, etc.

Donc voilà ce qui est apparu dans le communiqué du GAC. La première, il y avait une annexe 1 du communiqué du GAC. La deuxième partie concernait les nouveaux gTLD, et cela incluait comment les registres pouvaient s'occuper de questions de sécurité, comment ils pouvaient en informer l'ICANN. Nous voulons donc faire un suivi de cet avis pour voir l'efficacité de cet avis. Justement s'il y a eu des rapports et si cela a eu l'effet escompté.

La dernière partie de l'annexe 1, dont nous espérons pouvoir vous parler, voilà pourquoi Maggy et Dave sont parmi nous aujourd'hui. Bon cette dernière partie, je vous disais, concerne le rapport de l'ICANN et comment il s'occupe de l'usage malveillant, comment ils font des enquêtes sur ces réclamations qui leur sont présentées, ces plaintes, et quels sont les messages transmis quant à la conformité contractuelle pour atténuer cet usage malveillant.

Voilà certains points, au point de vue du GAC et au point du PSCWG pour parler de tout cela aujourd'hui.

CATHRIN BAUER-BULST: Et aujourd'hui, nous allons aborder les présentations. La première sera faite par Greg Aaron de l'anti-hameçonnage.

GREG AARON: Je représente le groupe de travail anti-hameçonnage. Je suis l'un des principaux chercheurs. Le APWG est l'une des principales entités s'occupant des recherches, de l'éducation, et de l'aide aux entités privées et publiques s'occupant du cyberdélit, le logiciel malveillant, le hameçonnage et le vol d'identité.

Je suis chercheur, je travaille avec Ithreat Cyber Group et je suis membre aussi du SSAC au sein de l'ICANN.

Donc voyons un tout petit peu comment cela fonctionne… bon, excusez-moi, je vous demande de bien vouloir passer à la prochaine diapo.

Voilà l'information du groupe de travail anti-hameçonnage concernant le hameçonnage enregistré depuis 2009. Vous pouvez voir que cette ligne rouge monte de manière constante.

En 2016, nous avons enregistré plus d'un million d'attaques de hameçonnage pendant l'année.

Ce que nous voyons, c'est que l'on fait beaucoup d'activités de hameçonnage et qu'il y a beaucoup de noms de domaine qui sont concernés par ce hameçonnage.

Si nous regardons 2009, nous avons vu qu'il y avait presque le double des tentatives d'hameçonnage que celle de l'année précédente.

Et cette année, les tentatives de hameçonnage étaient liées à une bande appelée « avalanche Gang ». Mais cette équipe a fait le travail depuis 2008 jusqu'en 2016. Ils ont été arrêtés le 13 novembre de l'année dernière. Et ce que je veux signaler, c'est que le groupe a pu faire son travail pendant très, très longtemps. Au cours des dernières années par exemple, ils ont volé 6 millions d'euros rien qu'en se portant sur une banque en ligne en Allemagne.

Mais ils ont beaucoup de cibles ailleurs en Europe et dans d'autres pays du monde. Les pertes totales se sont montées à des centaines de millions d'euros.

La prochaine image.

Ici, nous avons une partie de la réalité dont nous devons nous occuper lorsque nous parlons de cyber-délits et du système de noms de domaine.

Lorsque Avalanche a commis ces délits – bon vous savez que beaucoup de ces délits sont des délits professionnels – et Avalanche avait un réseau zombie qu'ils avaient loué à une autre bande de délinquants. Et il y a des services que certaines bandes de délinquants vendent à d'autres bandes de délinquants. Parce que ce qu'ils cherchent c'est le gain.

Un autre point que nous voyons, c'est que l'usage malveillant tend à se concentrer dans certains espaces de l'espace des noms de domaine. Et avec le temps, ils se déplacent d'un point sur l'autre.

Il y a beaucoup de domaines enregistrés avec certains bureaux d'enregistrements ou sous certains TLD. Les activités étaient hébergées chez certains fournisseurs d'hébergement. Donc l'une des choses concerne justement la raison pour laquelle les problèmes se produisent là où ils se produisent.

L'une des réponses c'est que les délinquants aiment bien se situer là où ils peuvent travailler sans être dérangés, où ils pourront travailler aussi longtemps que possible sans qu'on les interrompe. Là où il y a quelqu'un qui ne fait pas attention à ce qu'il se passe, ou qui ne fait pas attention à ses clients. Et cela se rapporte à l'espace des noms de domaine.

Parfois, c'est un manque d'attention, parfois il s'agit de prix qui sont très bas, et bien sûr ils veulent continuer à avoir ces gains, et ils veulent éviter le radar.

Il y a d'autres aspects liés à l'infrastructure. Parfois ce sont eux qui sont les propriétaires de cette infrastructure. Cela se passe dans certains services et avec l'espace des noms de domaine, il y a beaucoup de bureaux d'enregistrements qui en fait sont achetés par les délinquants. Ces bureaux sont la propriété de

délinquants qui ont été ensuite arrêtés pour avoir commis un cyber-délit. Et les bureaux d'enregistrement avaient reçu des contrats pour tuer des partenaires par exemple. Donc ces gens-là existent.

Une partie de cette atténuation ne se fait pas dans l'espace par les organismes d'application de la loi. Mais il y a certaines limitations en termes de ressources. Chaque organisme de l'application de la loi peut travailler dans sa propre juridiction, ce qui implique que l'on établisse une coopération avec des collègues dans d'autres juridictions et cela prend du temps.

Parfois les procureurs ne veulent pas s'occuper de dossiers dont ils savent qu'ils ne vont pas avoir des résultats positifs.

Donc le cyber-délit international travaille à l'encontre de l'application de la loi. Donc nous analysons un espace où les parties privées essayeront de maintenir les choses en ordre.

Donc il s'agit de leur demander de protéger leurs clients d'eux-mêmes et qu'ils passent des contrats pour cela. La révision contractuelle doit être renforcée par cela. Vous voulez utiliser Google ou Facebook, d'accord, nous allons passer un accord ou un contrat de termes de services. Et il faut le respecter ce contrat-là. Bien sûr, ces contrats couvrent bien sûr l'hébergement, et tout le reste.

C'est là que ces contrats permettent d'essayer d'éviter ou d'en finir avec ces activités délictuelles.

Les délinquants savent parfaitement comment cela fonctionne et ils ne respectent pas et ils ne travaillent pas en respectant nos normes.

Ici, nous avons quelques données de réputation d'une entreprise appelée SURBL. L'idée est de protéger votre navigateur, votre adresse électronique. Voilà l'information qu'ils publient, ils établissent une liste de noms de domaine qui ont une certaine réputation. La première, bien sûr le premier TLD c'est .COM, puisque .COM possède 140 millions de points de domaines.

.TOP est la deuxième. C'est un nom de domaine beaucoup plus réduit parce que vous n'avez que 4,6 millions.

Le troisième c'est .SCIENCE qui représente 250 000 noms de domaine à l'heure actuelle, ce qui signifie que la moitié des TLD constitue un problème, au moins pour ce fournisseur.

Et nous pouvons voir ici donc où se trouvent ces données .

Alors pourquoi ils sont groupés dans ce type d'espace. Qui est-ce qui vend ces domaines ? Qui est-ce qui utilise ces domaines ?

À mon avis, et du point de vue de la communauté de la sécurité, nous voyons ce qui suit. L'ICANN a un rôle à jouer en ce qui concerne la flexibilité, la résilience et la stabilité. Il y a un intérêt public et une différence sur la manière de comprendre l'intérêt public. Mais en définitive, tout le monde veut un internet stable et sûr pour le public.

C'est l'ICANN qui enregistre les bureaux d'enregistrements. Et la communauté a fait quelques contributions par rapport à ce que dit le contrat.

Certains outils dont nous disposons pour aborder ce type de problème concernent les dispositions d'exactitude du WHOIS. Il s'agit de dispositions du contrat contre l'usage malveillant d'enregistrement des données d'enregistrement. Et il y a aussi certaines responsabilités des bureaux d'enregistrements pour donner une réponse et un rapport de ces usages malveillants.

S'il y a des contrats, comment est-ce qu'on peut s'en servir ?

LA question est de savoir comment l'ICANN peut se servir de ces éléments et exécuter ces contrats.

Comme je l'ai dit, nous nous sommes centrés sur le fait d'utiliser ces éléments pour pouvoir résoudre les problèmes les plus graves. Parce que c'est gens-ci, en face, sont concentrés dans certains domaines et, en tant que responsable de sécurité, ce

qui m'inquiète, c'est la répétition des mêmes problèmes aux mêmes endroits. Ce qui se répète donc et qui devient de plus en plus important.

Alors que faisons-nous pour aborder ce problème, comment faisons-nous pour que les parties responsables puissent rendre des comptes et puissent se rendre responsables de ce qu'elles font ?

CATHRIN BAUER-BULST: Après cette présentation, nous allons faire une pause et nous aurons des échanges, des questions et des réponses avec vous. Vous pouvez participer avec le micro qui est ici, dans le couloir du milieu. Nous vous demandons de vous identifier, de faire le commentaire ou de poser la question que vous voulez poser.

Après avoir écouté la présentation, je vois certaines difficultés que nous pouvons rencontrer lorsque nous parlons d'atténuation de l'usage malveillant du DNS.

Est-ce qu'il y a des bonnes pratiques ? Ou une meilleure pratique pour savoir qui est capable de mieux atténuer, ou qui est-ce qui a eu du succès dans cette atténuation de l'usage malveillant.

GREG AARON: Ce n'est peut-être pas visible pour la communauté, parce que ces activités se font au quotidien. C'est quelque chose, si vous voulez, de régulier. Les bureaux d'enregistrement, les registres, reçoivent l'information, parfois par l'intermédiaire des organismes de contrôle, et les noms de domaine sont suspendus par centaine ou par millier chaque jour.

Dans certains aspects, les choses fonctionnent très bien, mais cela exige que toutes les parties reçoivent une communication, et qu'elle soit prête à faire ce qu'elles doivent faire.

Bon nombre de ces problèmes ne se rapportent pas aux personnes faisant partie de la réunion de l'ICANN, mais justement avec ceux qui ne viennent pas dans la réunion de l'ICANN.

Il y a beaucoup d'histoires réussies, mais la recherche nous a pris 4 ans, et nous savions auparavant qu'il y avait des problèmes qui apparaissaient. Mais le groupe a vérifié 1 million – pardon a fait un usage malveillant d'un million de noms de domaines, et je ne parle que de cette bande appelée Avalanche. Ils ont pu, donc profiter de tous ces noms de domaine dans le registre et obtenir davantage de choses.

CATHRIN BAUER-BULST: Merci Greg. Ceux qui sont face au micro maintenant.

JIM PRENDERGAST: Je vais dire quelque chose de facile pour commencer. Ceci ne se trouve pas sur le site web de la réunion. Pourrions-nous disposer de cette information ?

CATHRIN BAUER-BULST: Oui, c'était facile la première question.

SHANE TEWS: Une question pour Maguy parce que moi j'ai été dans la réunion précédente d'aujourd'hui. Greg a de bonnes données analytiques.

Je pense que la conformité contractuelle doit conserver la confidentialité des personnes, mais il faut que nous sachions quels sont les problèmes. Greg a dit que ces gens-là ont commencé par le hameçonnage et ensuite ils ont continué avec l'usage malveillant. Donc l'idée est de savoir que c'est toujours le même groupe de gens, pour que les gens qui s'occupent de l'application de la loi puissent les punir pour ainsi dire.

Vous ne pourriez pas nous donner quelque chose, des données plus précises ? Nous ne recherchons pas des noms spécifiques, des cas particuliers. Il faut voir la tendance qui se pointe là, pour que l'on puisse demander aux organismes d'application de la loi

que les gens se plaignent, qu'ils font des réclamations et pour que l'on sache quelle est la tendance pour que ce soit utile pour tout le monde.

MAGUY SERAD: Merci pour cette question. Je vais commencer par la fin. Il y a un moyen de faire un suivi de ce que nous appelons les rapporteurs, c'est-à-dire les gens qui signalent des problèmes à l'ICANN.

S'il y a un problème qui a été indiqué par une partie contractuelle et qui constitue un abus par rapport au système, nous avons la possibilité de vérifier cela.

Maintenant, je commence par le début de votre question, en ce qui concerne la possibilité de rentrer plus dans le détail en ce qui concerne les plaintes que nous recevons, je pense que c'est une des recommandations que nous avons eues de l'équipe CCTRT. Et donc nous travaillons, nous avons mis à jour notre rapport et nous travaillons avec l'équipe CCTRT pour mieux comprendre ces exigences, ces recommandations, et voir comment nous pouvons vous fournir ce niveau de détail que vous souhaitez.

CATHRIN BAUER-BULST: Merci Maguy. Nous avons Megan et puis le monsieur qui se trouve ici dans la salle.

MEGAN RICHARDS: J'ai mon propre micro, je ne dois pas me lever, ce qui est bien. Je suis Megan Richards, je représente la communauté européenne au sein du GAC, et j'allais vous poser une question par rapport à l'équipe CCT que vous avez déjà abordé.

Ma question concerne la liste que vous avez montrée par rapport aux cas de hameçonnage. Je pense que ce qui importe de cela est le poids relatif de tous ces différents dossiers. Alors que les numéros ont un impact assez important.

Je me demande, à partir de vos données, est-ce que vous voyez une distinction entre les ccTLD, les nouveaux gTLD, et les TLD historiques? Je pense que Drew est là aussi, parce que l'équipe CCTRT se penche aussi sur les études qui ont été faites sur les abus du DNS. Et je pense que ce sont des informations importantes pour voir quelles sont les mesures qui peuvent être mises en place au niveau des ccTLD nationaux par exemple, ou dans d'autres environnements.

GREG AARON: Je travaille en ce moment sur un document qui sera publié le mois prochain en coopération avec d'autres chercheurs.

Nous allons détailler toutes les activités de hameçonnage qui ont eu lieu en 2015 et 2016 et en les divisant par catégories. Il

s'agit de beaucoup d'informations, mais nous espérons qu'il s'agira d'une publication définitive sur les deux dernières années.

Nous allons voir donc à ce moment-là ce qu'il s'est passé réellement. Ce document sera publié dans un mois et aura donc une différenciation des chiffres en termes de ccTLD et gTLD.

CATHRIN BAUER-BULST: Nous allons prendre une autre question et après, nous allons arrêter pour laisser la place aux autres présentations.

NON IDENTIFIE: Merci beaucoup pour ces informations. C'est des informations qui ne sont pas très prometteuses. Et les présentations sur les cas d'abus de l'année 2015 concernent des millions, ce qui ne nous rend pas très heureux.

Et je suppose, à partir de ce que vous avez montré, que la façon d'atténuer le risque de ce type d'abus dépend du secteur privé plus que des autorités juridiques.

Comme vous le savez tous, les abus, malheureusement, n'ont pas lieu, les cas d'abus ne viennent pas d'amateurs, mais plutôt de gens qui ont beaucoup d'expériences.

Je me demande donc quel est le rôle des autorités en tant que leader pour prendre soin de cette atténuation des risques d'abus.

GREG AARON : Dans certains cas, les délinquants enregistrent les noms de domaine et les utilisent le jour même. C'est très rapide pour que les forces de l'ordre puissent s'en occuper tous les jours.

Ils doivent se concentrer sur certains cas dans une période de temps.

Il s'agit de problèmes qui ne sont pas nouveaux. Les entités privées, les opérateurs de réseau et les fournisseurs de services internet sont confrontés à ce problème depuis longtemps. Parce qu'ils sont les seuls qui peuvent apporter une solution.

Quand on voit que ces problèmes se reproduisent, c'est à ce moment-là que l'on se dit : qu'est-ce qu'on peut faire ? Et cela concerne aussi le département, par exemple, de la conformité contractuelle.

Le délit bouge de manière très rapide, agit de manière très rapide. C'est pour cela qu'il est tellement difficile de le suivre, de suivre.

CATHRIN BAUER-BULST: Je vous demande de parler lentement pour les interprètes et d'être concis pour que tout le monde puisse avoir la possibilité de parler.

WERNER STAUB : Je viens de CORE Association. Je vais faire référence à la liste que vous avez montrée par rapport aux TLD qui ont fait l'objet de beaucoup d'abus.

Deux de ces noms de domaine que j'ai vu sur cette liste viennent d'une partie qui a fait l'objet d'un dossier de révision indépendante de l'ICANN. Est-ce qu'on pourrait avoir un peu plus de détails par rapport à cela ?

Si cette partie peut gagner une procédure contre l'ICANN, qu'est-ce qui se passerait ?

CATHRIN BAUER-BULST: Merci pour cela. Est-ce que vous voulez répondre ?

DENISE MICHEL: Denise Michel de Facebook.

Greg, j'aimerais revenir sur le dernier point que vous avez évoqué, pour voir si vous pouvez nous expliquer un petit peu plus dans quelle mesure les obligations contractuelles sont utilisées de manière efficace pour lutter contre cette tendance

assez importante de cyber-délinquance dans les gTLD. Et si ce n'est pas le cas, quelles sont vos suggestions.

GREG AARON: Je pense que c'est une question qui concerne plutôt Maguy. Mais ce que je vois, à partir de mon travail, c'est que par exemple les bureaux d'enregistrements qui ont des centaines de milliers de noms et qui ont des informations fausses dans leur WHOIS. Cela ne veut pas qu'il y a de la mauvaise fois de la part des bureaux d'enregistrement, et ensuite, on doit voir ce qu'il se passe avec ces noms de domaine, et ensuite il faut voir si ces comportements se reproduisent.

NON IDENTIFIE: Bonjour (Carlos). Greg nous a montré des informations. Nous essayons donc à partir des informations comme celles qu'il a montrées de voir quel est le poids de chacun des TLD et puis nous voyons beaucoup de différences entre les ccTLD, les TLD historiques et les nouveaux gTLD.

Il y a beaucoup de différences entre ces types de TLD.

Est-ce qu'on peut expliquer cela ? Je pense que cela nous montre qu'il y a encore beaucoup d'améliorations que l'on peut apporter.

CATHRIN BAUER-BULST: Est-ce que vous pouvez nous dire quelles sont les différences que vous voyez ?

NON IDENTIFIE: Si on voit les ccTLD traditionnels, on va voir qu'ils ont des politiques plus strictes au niveau de l'enregistrement. Par exemple vous devez habiter dans un certain pays pour pouvoir enregistrer un ccTLD, alors qu'il y a d'autres TLD qui sont ouverts à tous.

Ensuite il y a la différence de prix. Les domaines qui sont moins chers attirent plus les délinquants, parce que les délinquants cherchent le profit, et donc ils font leurs activités et ensuite ils abandonnent. Donc ils essayent de dépenser le moins possible.

DREW BAGLEY : Bonjour, Drew Bagley, de la Sécurity Domain Foundation. Maguy a parlé de l'équipe CCT, et j'aimerais vous parler de ce que nous faisons dans cette équipe en ce qui concerne les cas d'abus.

Demain, nous aurons une séance où l'on va parler de l'étude sur les abus du DNS qui a été réalisée et nous allons nous pencher sur les cas d'abus dans les TLD versus les nouveaux TLD, les TLD historiques versus les gTLD. Donc si vous pensez que vous

pouvez contribuer à cette discussion, ou si vous pouvez faire des commentaires par rapport aux méthodologies de luttes contre la cyber-criminalité, vous êtes les bienvenus.

CATHRIN BAUER-BULST: Merci beaucoup. Nous allons clore les questions ici. Et nous allons passer à la prochaine présentation. Permettez-moi de vous rappeler que sur Adobe Connect, vous avez la transcription qui est disponible.

BOBBY FLAIM : Est-ce que vous pourriez poser votre question après la prochaine présentation ? Merci.

Alors, on aura 5 minutes de présentations, et ensuite on aura des questions concernant cette présentation spécifique. Et ensuite, à la fin, nous aurons plein de temps pour poser d'autres questions.

Très bien.

Merci Greg de ta présentation. Nous voyons beaucoup de tendances. Et il faut penser donc aux moyens efficaces de pouvoir comprendre ces tendances au niveau des entreprises et voir comment nous pouvons être plus efficaces.

Je vais donc présenter notre prochain présentateur. Il s'appelle Graig Schwartz, il est co-fondateur du Verified TLD Consortium, et il est aussi registre de .BANK ; Graig, si vous êtes là, est-ce que vous pouvez prendre la parole ?

CRAIG SCHWARTZ: Oui, je suis là.

BOBBY FLAIM: Nous vous entendons très bien.

CRAIG SCHWARTZ: Je suis ravi de participer à cette séance et de partager notre expérience dans l'opération des noms de domaine .BANK pour prévenir le cyber-délit.

Nous avons des restrictions à l'enregistrement qui visent à atténuer les risques d'abus dont vous allez parler aujourd'hui.

J'essaye de vous montrer les diapos au fur et à mesure que je parle.

BOBBY FLAIM: Merci, dites-nous quand vous voulez que l'on change de diapo.

Craig, je pense qu'on a des difficultés pour montrer vos diapos. Je vous prie de continuer, et ensuite on va essayer d'afficher les diapos.

CRAIG SCHWARTZ: En tant qu'opérateur de registre, nous nous efforçons de développer des politiques qui visent à protéger nos communautés, ainsi que les consommateurs.

Nos politiques sont élaborées par les représentants de la communauté financière, ainsi que par des experts en matière de sécurité et en opération de DNS.

L'intégrité de .BANK et .ASSURANCE est préservée tout d'abord grâce à nos politiques qui définissent très strictement les critères d'éligibilité pour pouvoir enregistrer des domaines sous .BANK et .ASSURANCE ; de cette manière, seules peuvent enregistrer ces domaines les personnes qui peuvent prouver avoir remplis les conditions d'éligibilité établies dans nos politiques. Ces politiques font références aussi aux cas d'abus.

Ensuite, je parlerai des vérifications des titulaires de noms plus tard dans ma présentation.

Comme je vous disais, ces exigences ont été développées par une communauté, par un groupe de la communauté. Et nous faisons donc un suivi des infractions que nous pouvons

identifier. Nous avons une interaction en ce qui concerne les services d'enregistrement fiduciaire et d'anonymisation.

En ce qui concerne la vérification des titulaires de noms, et c'est un élément clef pour nous, nous envisageons de faire ces vérifications avant tout enregistrement du nom de domaine, afin de nous assurer que le titulaire possède donc les compétences, ou qu'il est éligible.

En 2014, nous avons lancé un appel à propositions et nous avons reçu un certain nombre de réponses pour mettre en place un service de vérifications.

Quand Bobby et moi nous parlions de cette séance, il m'a demandé si nous pouvions partager des informations par rapport au coût que cela représente, le fait de faire vérifier par une tierce partie les enregistrements. Les propositions des fournisseurs partaient de 80 USD à 104 (40 ?) USD par titulaire, et parfois un peu plus cher.

En plus de cette vérification des titulaires, nous avons aussi un certain nombre d'exigences, telles que la validation DNSSEC, l'authentification de la messagerie électronique. Cela est très détaillé dans les informations qui figurent sur notre site web.

Comme je l'ai dit avant, le fournisseur de vérification s'assure que toutes les exigences sont respectées.

Les restrictions à l'enregistrement et la vérification des titulaires sont des éléments clefs pour assurer l'intégrité de ces noms de domaine .BANK et .ASSURANCE, afin que le public puisse faire confiance à ces noms de domaine.

Cela fait deux ans que nous sommes en fonctionnement, et nous n'avons eu aucun cas d'abus lié à l'utilisation de .BANK et .ASSURANCE.

Nous pensons qu'il est important de développer des ressources pour faire comprendre aux titulaires quelle est la valeur que nous proposons dans nos TLD et pour les aider à mieux utiliser leur nom de domaine.

Et bien sûr, les titulaires utilisent nos noms de domaine et de cette manière, ils peuvent comprendre quelle en est la valeur ajoutée pour eux.

Ensuite, je vais revenir sur un élément. Comme je vous ai dit, les coûts opérationnels sont plus importants pour les services de registre, et peut-être que vous seriez intéressés à savoir quel est ce coût. Et celui-ci va d'une centaine à 1500 USD par domaine, par an. En fonction de ce que le bureau d'enregistrement ou le titulaire de nom utilise, et en fonction des types de titulaires qui achètent ce type de noms de domaine.

Nous sommes un groupe de noms de domaine de premier niveau, parmi lesquels figurent .PHARMACIE, .NET, .REAL qui travaillons en faveur de la confiance du public en ligne dans nos différents TLD.

Dans la séance du groupe de travail qui aura lieu demain, du groupe de travail qui s'occupe de la sécurité à 6 h 30, des représentants de mon entreprise vont vous parler de ces activités.

Et avant de terminer, il y a des ressources que vous voyez sur l'écran, que je vous invite à visiter.

BOBBY FLAIM: Est-ce qu'il y a des questions pour Graig ? Très bien, nous avons une question.

JOHN LEVINE: Bonjour, John Levine. Vous avez dit qu'il y avait 6 000 titulaires, mais j'ai vu qu'il y avait 2900 noms sous .BANK et .ASSURANCE, alors où sont partis les autres ?

GRAIG SCHWARTZ: Bonne question John. Deux des exigences pour les noms de domaine concernent la validation DNSSEC et donc ces noms doivent utiliser des serveurs de noms qui apparaissent dans la

zone de .BANK. Donc pour les noms de domaine des titulaires qui n'ont pas répondu à ces enregistrements, leurs domaines n'apparaissent pas dans cette zone-là.

JOHN LEVINE: Ok. J'ai vu que vous avez parlé de .PHARMACIE et .DOCTEUR, et ce sont des secteurs réglementés aussi. Est-ce que ce modèle va au-delà, pour vérifier qui est éligible ?

CRAIG SCHWARTZ: Je ne peux parler que pour .BANK et .ASSURANCE et un des éléments pour ce qui est de la valeur ajoutée de ces TLD, c'est le fait que ces entités sont légitimes dans notre espace.

Je suis sûr que ce modèle pourrait fonctionner dans d'autres espaces, mais je n'en suis pas sûr à 100 %.

BOBBY FLAM: Michèle.

MICHELE NEYLON: Bonjour Graig, comment allez-vous ?

Je pense que la question ici et l'échelle et le prix. Avec ce type de politiques en cours, vos domaines seront disponibles pour un sous-groupe très petit de titulaires, que ce soit des organisations

ou des individus. Alors, à bien des égards, en tant que modèle je ne vois pas comment on pourrait l'appliquer à grande échelle pour le grand public. Ou bien je n'ai pas compris quelque chose.

CRAIG SCHWARTZ: Je ne suis pas très sûr de ce que vous voulez dire par votre commentaire quand vous dites qu'on ne peut pas le développer à grande échelle.

MICHELE NEYLON: Je vais être plus précis. Ce que vous faites coûte une fortune. Donc pour enregistrer ces noms de domaine, le coût sera significativement que pour d'autres TLD. Et donc les gens qui pourront enregistrer ces noms de domaine sont ceux qui pourront payer un prix très élevé. Et c'est pourquoi cela deviendrait accessible aux gens qui auront cet argent à payer.

Voilà ce que je voulais dire.

CRAIG SCHWARTZ: Vous avez tout à fait raison. Et une partie de l'attrait de ces TLD, c'est l'exclusivité et c'est parce qu'ils sont accompagnés de la certitude qu'il s'agit de TLD légitimes.

BOBBY FLAIM: Merci beaucoup. Est-ce qu'on a d'autres questions pour Craig ? Très bien, nous pouvons passer à la présentation suivante.

Mais j'ai une question moi-même. Nous avons déjà posé cette question à Craig pour voir comment cela pourrait fonctionner dans tous les noms de système. Nous avons entendu cet argument selon lequel il est très difficile d'appliquer ce modèle à grande échelle. Et Michèle et moi- même, nous avons eu cette discussion. Quand ont pense aux fonds provenant des enchères, est-ce que l'on pourrait utiliser ces fonds pour ce type d'initiative ou ce type d'effort ?

Je n'ai rien de spécifique, mais la lutte contre les abus va coûter de l'argent. Alors lorsqu'on pense à ces fonds, comment pourrait-on les affecter à la vérification par exemple des titulaires, ou à des actions qui puissent nous aider à mieux atténuer ces risques à travers la communauté.

C'est une discussion à part, et notre prochain présentateur, c'est David Conrad, le CTO de l'ICANN.

DAVID CONRAD: Merci Bobby. La prochaine image. Je dois dire que mon équipe de la direction technique a fait un travail de recherches, aussi bien que des activités de résilience, de sécurité et de stabilité. John Crain, qui est ici dans la salle, est le directeur par rapport à

la résilience, la sécurité et la stabilité. Et c'est son équipe qui a fait une enquête, une recherche sur ce que je vais aborder dans cette présentation.

Je vais parler de la manière de gérer l'usage malveillant et l'abus, avec la conformité contractuelle et les parties contractantes et d'autres.

Nous allons parler du projet de recherches sur la recherche publique de l'utilisation malveillante et la technologie pour améliorer l'atténuation de l'usage malveillant.

Nous allons parler de l'équipe SSR et son interaction avec la conformité contractuelle. L'équipe de SSR et la conformité contractuelle font des recherches pour améliorer la collaboration qu'ils ont.

Vous savez qu'on a un nouveau chef de la conformité contractuelle et un nouveau département au sein de l'ICANN. Nous avons discuté de la manière dont nos équipes peuvent donner un soutien plus important à la conformité contractuelle en ce qui concerne les différents aspects des activités que le département, le service de conformité contractuelle doivent mener à bien.

L'équipe SSR doit présenter les problèmes. Bien sûr, nous ne faisons pas de conformité contractuelle, mais lorsque nous

détectons des points un peu bizarres, nous transférons ce problème à l'équipe de conformité contractuelle pour qu'ils fassent des recherches.

L'équipe SSR s'entretient avec la conformité contractuelle et l'aspect opérationnel pour permettre une collaboration informelle dans l'atténuation des menaces.

Mon équipe et celle de John participent à différents groupes de confiance du consommateur et ces équipes de confiance du consommateur fournissent une information confidentielle qui est échangée et qui permet à nos équipes de découvrir les différents problèmes qui ont pu apparaitre pour utiliser nos connaissances et pour justement atténuer les problèmes dans la mesure du possible.

Nous avons aussi un projet de recherche contre l'usage malveillant dans l'équipe SSR. Nous avons un sous-traitant qui fait une analyse de l'usage malveillant, une analyse qui est en phase bêta. Nous obtenons différents types de données, différentes modalités d'usages malveillants pertinents dans le contexte du communiqué du GAC.

Dans ce contexte, dans ce communiqué, on parle du hameçonnage, des réseaux zombie et d'autres que nous avons ajoutés en plus de ce que le communiqué du GAC mentionnait. Parce que nous avons estimé qu'il s'agissait d'indicateurs très

appropriés, même si nous ne pouvons pas les aborder directement.

L'idée est de voir comment nous pouvons présenter ces résultats au public. Les données que nous recevons sont considérées comme des données privées qui sont en plus protégées par un accord de non-diffusion qui fait partie du contrat.

Voilà une capture d'écran de cette plateforme Beta. Je sais que la typographie est trop petite, que c'est difficile à lire, mais l'idée est la suivante. Ici vous avez un palmarès des TLD, cela inclut l'information sur les domaines dans la zone, le nombre de domaines qui se trouvent sur la liste, une qualification pour l'usage malveillant qui va de 1 à 10. Et donc on peut voir cette qualification avec les différents gTLD liés à l'utilisation malveillante pour ce cas particulier. Il s'agit de domaines inclus dans la liste par rapport au nombre total de noms de domaine.

Nous allons parler maintenant de la méthodologie d'atténuation des attaques d'usages malveillants au DNS.

Ce document a été créé comme réponse à l'une des recommandations de la première équipe de révision de la sécurité et de la stabilité et la résilience. Cette révision était obligatoire, et je crois qu'elle a eu lieu il y a 4 ans.

La recommandation 12 disait qu'il fallait créer une méthodologie d'atténuation pour les attaques des identificateurs.

L'équipe SSR a élaboré ce document, et là vous avez les étapes de haut niveau inclus dans cette méthodologie : identifier, donner la priorité et mettre à jour régulièrement la liste des attaques les plus importantes, développer une orientation de haut impact et les vulnérabilités dues aux risques, décrire les pratiques d'atténuation des attaques correspondantes et encourager l'adoption de ces pratiques par des contrats, des accords, des encouragements, etc.

Là vous avez l'adresse pour télécharger le PDF correspondant.

En ce qui concerne l'amélioration de l'atténuation de l'usage malveillant du DNS, l'équipe SSR doit donc des analyses et des données impartiaux, pour ainsi dire, pour que la communauté informée puisse élaborer des politiques tenant compte de cet usage malveillant.

Il y a aussi la question des aspects internes, l'organisation interne, avec différentes fonctions liées à l'usage malveillant du DNS.

Aussi bien l'équipe de SSR ainsi que le groupe de recherches aux CTO sont centrés sur ce type de points.

Pour améliorer les résultats de l'atténuation de l'usage malveillant du DNS, nous donnons des formations et notre avis à la communauté de la sécurité publique pour leur permettre de comprendre l'environnement du DNS au point de vue technique, les processus d'élaboration des politiques de l'ICANN et quels sont les processus et les procédures organisationnels au sein de l'ICANN elle-même.

Et maintenant, je vais céder la parole à Maguy.

BOBBY FLAIM: Pourriez-vous projeter les diapos de Maguy ? C'est celles que l'on voit là ?

MAGUY SERAD: Bonjour à tous. Je m'occupe de la conformité contractuelle. Prochaine image s'il vous plait.

La demande spécifique du PSWG concernait le traitement de ces thèmes. Voilà le contexte et les antécédents et c'est la réponse à l'annexe 1 du communiqué du GAC.

Prochaine image maintenant.

La première question était la suivante : comment l'ICANN et l'équipe SSR de l'ICANN ainsi que le département de conformité contractuelle, comment font-ils pour travailler ensemble ?

Comme David l'a dit, l'équipe de la conformité contractuelle a différentes organisations internes dans l'organisation de l'ICANN. Et là, j'ai fait une liste de certains aspects, mais je veux mettre l'accent sur ce que David a dit.

Notre équipe a travaillé depuis le début avec l'équipe CCR sur tout ce qui concernait l'usage malveillant du DNS.

Nous travaillons comme cela. Nous recevons la présentation d'un problème que quelqu'un a vu et nous essayons d'obtenir autant d'informations que possible de ceux qui nous présentent le problème avant d'utiliser les éléments contractuels et de nous mettre en contact avec la partie contractante.

Toutes les obligations de conformité contractuelle suivent la même méthodologie.

Pour l'autre question, vous avez demandé quelles étaient les actions spécifiques ou les mesures spécifiques qui avaient été mises en pratique par rapport aux bureaux d'enregistrement.

Nous publions tous les rapports et tout ce que nous publions concerne les actions qui sont mises en œuvre contre les parties contractantes.

Pendant cette étape, nous mettons à la disposition du public l'activité d'exécution qui est en cours, pour quelle partie contractante. Et en plus du thème spécifique qui fait l'objet de

notre analyse, ce que nous faisons dans la conformité contractuelle, nous faisons une vérification de conformité contractuelle avant d'émettre un avis de non-conformité. C'est-à-dire quelle est la conformité généralisée de cette partie contractante, dans quels domaines il pourrait y avoir des manquements, et nous incluons tout cela dans l'avis de manquement, pour que tout cela fasse partie du même thème et que nous ne soyons pas obligés d'aborder à chaque fois une chose. Ceci fait partie de notre mémoire.

En 2016, nous avons eu 4 bureaux d'enregistrements qui ont reçu cet avis de manquement. La question est de savoir quelles sont les mesures que nous avons prises pour améliorer la conformité des bureaux d'enregistrement.

Moi j'ai beaucoup d'images à vous montrer mais, pour résumer, la meilleure façon de le faire est d'améliorer la conformité contractuelle, c'est de faire des activités que l'équipe de la conformité contractuelle puisse mettre en place.

Nous analysons l'état de l'univers contractuel où nous voyons apparaitre les tendances. Nous voyons la cohérence entre les thèmes et les occasions qui se présentent pour faire de la diffusion, de la sensibilisation. Et il faut voir si cette diffusion se fait pour le secteur public ou une autre partie contractante en particulier.

Il s'agit donc d'une image plus vaste des efforts de sensibilisation de notre part, mais aussi pour améliorer la conformité.

S'il y a un problème que nous avons par exemple, déjà abordé par le passé, et que nous voyons que le problème se représente, nous allons avoir un avis d'escalade avec la partie contractante, parce que cela signifie que s'il n'a pas résolu le problème avec la partie précédente, il va devoir le faire avec celui-ci.

En ce qui concerne la conformité aussi, nous améliorons cet aspect avec les audits proactifs que nous avons à réaliser. C'est une manière proactive d'identifier les problèmes, de les aborder, d'essayer de les atténuer, pour éviter qu'ils ne se répètent.

Voilà quelques données, je ne vais pas analyser dans le détail chacune des diapos.

Vous avez ici les détails qui donnent les fondements de notre réponse au communiqué du GAC. Cela se rapporte à 32 000 réclamations entre novembre 2015 et novembre 2016. Sur la base de la conversation que nous avons eue, on a voulu savoir comment ils avaient été ventilés. Combien on en avait reçu, combien on avait pu en résoudre, etc.

Ce que je veux signaler c'est que dans ce tableau que vous voyez sur l'écran, nous avons résolu le nombre de cas que vous voyez

sur la gauche. Mais il faut que vous voyiez aussi, et que vous fassiez attention au fait que nous avons révisé les réclamations avant de les envoyer aux parties contractantes.

Et vous pouvez voir qu'il y a une colonne qui dit : clôturé, ou fermé avant le premier avis. Et pourquoi ? Parce que parfois nous avons des réclamations qui ne sont pas complètes ou qui ne sont pas à la portée des réclamations qui nous ont été présentées, mais qui se rapportent à un nom de domaine qui a déjà été suspendu ou éliminé ou qui n'est plus valable.

Voilà pourquoi nous avons beaucoup de dossiers pour la fermeture et sa publication dans notre site web.

Ce que nous donnons au public aussi, et il ne le réalise pas non plus parfois, nous avons aussi un processus de résolution informel. Je veux attirer l'attention du public sur ce qui se passe entre la première, la deuxième et la troisième notification. Avant ce dernier avis de manquement. Quand on présente : voilà ce qui se passe avec le premier avis. Voyons un peu les absences d'exactitude de WHOIS. On en a presque 14 000. Dans la première notification. Et cela, qu'est-ce que cela nous dit ? cela nous dit que ce chiffre est bien moindre lors de la deuxième notification. Cela signifie que lorsque l'on a posé les problèmes, ils ont été résolus lors de la première notification.

Lorsque nous parlons d'une deuxième notification, nous parlons de 1340 cas. Qu'est-ce qui se passe si une partie contractante ne répond pas à un avis de conformité, nous allons donc aborder la prochaine étape. Si la conformité reçoit une réponse complète de cette partie contractante à la dernière minute, on passe à la deuxième étape.

Le message est ici, et c'est le suivant. De 14 000 nous sommes passés à 1300. Et en principe que l'on applique est le même pour la troisième notification.

Notre objectif est le suivant : les problèmes qui se posent par rapport à la conformité contractuelle auront dû être révisés, abordés et que l'on ait trouvé une solution pour ces problèmes. C'est ce à quoi on s'attend.

Je pourrais en parler un tout petit peu plus mais vous nous avez demandé davantage de détails à cet égard.

J'ai fini de toute façon.

Encore une… S'il vous plait Fabien, encore une diapo. Voilà.

C'est les activités de surveillances que nous mettons en place et je vous montre quelles sont les sources que nous utilisons quand nous faisons ces activités de surveillance.

Vous voyez donc les activités que nous avons mises en place en 2016, pour information, pour vous. Tout cela est disponible sur notre site web.

Avec ceci, je conclus ma présentation. Merci beaucoup.

BOBBY FLAIM: Merci beaucoup. Il nous reste 12 minutes et nous voulons savoir si le public a des questions ou s'il y a quelqu'un du panel qui souhaite intervenir. Oui monsieur ?

JOHN CARR: John Carr de l'alliance NGO Européenne pour la sécurité des enfants en ligne. J'ai été très intéressé à la première présentation qui a montré le niveau de vérification et de sécurité qui était mis en place pour vérifier l'identité des titulaires. Et je vais vous dire pourquoi.

Nous avons fait un suivi du processus de TLD pour .KIDS pendant un certain temps, c'est un problème qui n'est pas résolu comme vous le savez, mais il y a 5 mois on a su que ce .KIDS, il y a déjà un registre en Russie qui s'appelle .DJETI, qui correspond à enfant. Alors ma question est la suivante : quand vous mettez à la vente un tel nom de domaine, est-ce que vous avez par exemple une hypothèse des gens qui pourraient acheter un tel nom de domaine ? Et par exemple s'il s'agit de .KIDS, le fait de

vérifier que la personne qui achète ce titre de nom de domaine n'ait pas de casier judiciaire en ce qui concerne des délits contre des enfants.

Est-ce que vous faites ce type de vérification ? La réponse a été non, il n'y a pas de stipulation de ce type et il n'essaye pas de vérifier si ces exigences sont remplies ou non.

Alors je pense que l'ICANN n'a pas respecté ses obligations en matière de respect des enfants. Et je vois que si .KIDS est accepté et qu'il y a des problèmes en matière de sécurité, cela pourrait être lié aux inquiétudes que l'on a pu voir apparaitre dans des secteurs très règlementés.

C'est un commentaire général par rapport aux types d'actions qui pourraient être mis en place pour éviter ce type de problèmes.

DAVID CONRAD: Je ne suis pas très sûr de comment répondre à votre commentaire. Nous mettons en place des procédures associées à la prochaine série de candidatures. Et c'est bien sur un domaine sur lequel nous pouvons nous focaliser pour demander aux titulaires des informations supplémentaires.

En ce qui concerne les gTLD existants, je n'ai pas suffisamment d'informations ou de recul ou d'informations juridiques pour

savoir qui peut enregistrer ou non un nom de domaine. Et je devrais m'en remettre au département juridique pour obtenir une réponse.

CATHRIN BAUER-BULST: Nous avons une question à distance de Steve Metalitz pour Greg : merci Greg pour votre présentation, vous avez souligné l'importance des contrats, de l'exécution des contrats et des conditions de service. Cela implique aussi des engagements volontaires. Est-ce que vous avez des idées par rapport à cela ?

GREG AARON : Je pense que ce à quoi fait référence Steve, c'est aux marques enregistrées. Il s'agit d'un domaine très spécifique qui est différent de celui du cyber-délit.

Je pense que la question a été tranchée il y a un certain temps. À savoir que quand on travaille avec le cyber-délit, avec des cas de hameçonnages et de logiciels malveillants, il y a un rôle pour la communauté.

Steve fait référence donc aux marques déposées et cela concerne plutôt le domaine civil.

KEITH DRAZK: Bonjour à tous, je m'appelle Keith, je travaille pour VeriSign.

J'ai une question. Est-ce que vous vous penchez sur le problème qu'on appelle « domaine hopping »? C'est une pratique où les délinquants utilisent le système de noms de domaine et passent d'un TLD à un autre TLD, à un autre TLD. Ils sautent de TLD en TLD. Et cela a été identifié comme un type d'abus.

Vous avez dit Greg dans votre rapport qu'il y avait des dizaines, des centaines et des milliers de domaines qui étaient enregistrés. Et donc dans ce cas, les délinquants amènent leurs activités délictuelles d'un domaine à l'autre.

Est-ce que les acteurs de l'industrie peuvent communiquer et trouver des instances pour que ces délinquants puissent être identifiés dans un TLD en particulier, ou ccTLD, et pour essayer d'identifier ce mauvais comportement, le communiquer pour essayer de prévoir vers où va le délinquant. Ce qui pourrait d'ailleurs permettre de poursuivre ces délinquants à travers le monde.

GREG AARON: Merci pour cette question Keith. En ce moment, il y a 365 millions de domaines enregistrés dans le monde dans tous les registres.

Et comme vous le dites, pour les délinquants, les noms de domaine ce sont des ressources dont ils se servent et qu'ils

jettent par la suite. Ils enregistrent un nom de domaine, et ensuite ils s'en débarrassent.

Il devrait y avoir un effort de coordination pour essayer d'identifier ces gens. Ces gens utilisent aussi des identités fausses.

Nous devons donc nous assurer que nous avons accès aux informations. La disponibilité continue des informations du WHOIS est un sujet d'actualité à l'heure actuelle. Cette disponibilité d'information est un élément clef et je dois mettre l'accent sur cette information car sans ces informations, il est très difficile de pouvoir travailler. Il est difficile de retrouver ces délinquants.

C'est un travail qui est difficile du point de vue pratique, qui nécessite beaucoup de fonds.

CATHRIN BAUER-BULST: Une question. Je pense que c'est une bonne idée, on voudrait le voir dans d'autres contextes comme par exemple le contenu. Des contenus qui, par exemple sont suspendus dans certains domaines et qui réapparaissent dans d'autres sites, comme c'est le cas de contenus liés aux enfants.

Il est important donc de pouvoir avoir les moyens de comparer des images identiques qui ont été légèrement modifiées, et

comparer cela à travers la valeur [Hash]. De cette manière on pourrait stocker des informations sur les délinquants et peut-être que les fonds issus des enchères pourraient être consacrés à ce type de mesure.

Je vais passer aux trois prochaines questions, et ensuite nous allons clore cette séance. S'il vous plait madame.

JOYCE LIN: Joyce Lin, de 007names.com.

Je pense que ces données que vous avez montrées sont très intéressantes et, actuellement, l'application de la loi repose sur les titulaires de noms.

Très récemment, nous avons reçu un email d'une organisation qui fait le suivi des achats ou des ordonnances médicales sur internet. Et ils nous ont dit vous avez 12 noms de domaines qui vendent des produits pharmaceutiques. Nous essayons d'aider et nous leur avons envoyé donc une réponse en disant : nous avons eu cette réclamation par rapport à votre nom de domaine. Vous avez un contrat à respecter et conformément à l'application du contrat RAA, nous devons vous donner 15 jours pour corriger cette action. Et dans deux heures ce domaine avait disparu.

Alors qu'est-ce que l'on peut faire ? En tant que bureau d'enregistrement nous avons perdu un client, mais entre-temps, nous n'avons résolu rien.

Alors moi je me suis sentie un peu idiote, parce que j'ai perdu un client, mais en même temps je n'ai aidé personne. Je n'ai pas aidé à résoudre le problème.

Je pense que l'ICANN devrait envisager d'autres moyens de placer cette tâche ou ces actions pour lutter contre les abus.

Je pense que ce poids devrait reposer sur le registre, et non pas sur le titulaire, sur les bureaux d'enregistrement. Il y a d'autres domaines que nous ne pouvons pas renouveler, que nous ne pouvons pas revendre. Et les clients ne veulent pas payer pour cela parce qu'ils sont bloqués.

Comment nous savons lorsqu'il s'agit de ce blocage de nom de domaine, combien ça va durer, parce que quelqu'un doit payer pour cela.

La question est de savoir si l'ICANN ou une autre autorité ont identifié un nom de domaine, devrait s'adresser au registre en leur disant : tous ces noms doivent être en dehors du fichier [nn], ce serait plus efficace de faire cela.

Autrement, vous n'avez pas besoin de sauter de TLD à TLD, il suffit de sauter de bureau d'enregistrement en bureau d'enregistrement.

Merci.

BOBBY FLAIM : Je pense que votre question rejoint celle Keith. Est-ce qu'il y a un moyen de pouvoir nous assurer qu'il y ait une liste par exemple de délinquants pour essayer qu'ils soient maintenus en dehors du DNS ? Est-ce que cela semble possible ?

DAVID CONRAD: La joie de l'internet, c'est que quand vous êtes sur internet, personne ne sait qui vous êtes. Personne ne sait que vous êtes un criminel.

Beaucoup de ces problèmes sont très difficiles à identifier en termes de solutions. L'organisation ICANN repose sur la communauté qui nous aide à identifier des mécanismes pour pouvoir apporter une réponse aux problèmes qui nous affectent tous.

En ce qui concerne ce domaine hopping, il peut y avoir des moyens pour partager les informations et de trouver des techniques qui puissent nous suggérer les domaines plus

susceptibles d'être attaqués par ce type de délits. Et que ces informations puissent revenir au registre, aux bureaux d'enregistrement pour identifier des vulnérabilités potentielles.

Mais qu'est-ce qu'on fait avec ces informations ? Bloque-t-on ces domaines ? Alors que cela peut être compliqué. Les registres versus les bureaux d'enregistrement, c'est un autre sujet aussi.

Mais il s'agit de domaines où la communication pourrait être améliorée, comme par exemple la notification de changement, etc. C'est un aspect. Nous nous penchons avec nos équipes, voir comment nous pouvons éviter ou travailler pour partager les informations que nous collectons dans l'organisation et partager cette information avec la communauté pour essayer de trouver des moyens de répondre à ce type de difficultés.

Ce n'est pas une réponse que nous allons trouver bientôt, mais j'espère que cela pourra aider la communauté dans ses délibérations.

CATHRIN BAUER-BULST: S'il vous plait, allez-y.

KAVOUSS ARASTEH: Bonjour, je suis Arasteh, je suis membre du GAC. J'aimerais apporter une vision différente à cette situation. Je pense que

nous sommes en train de regarder ce problème de manière un peu fragmentée, et que nous ne voyons pas les choses dans le long terme.

Il y a eu des mesures qui ont été mises en place pour atténuer ces risques, mais qui ne semblent pas être en mesure de rattraper la vitesse de ces délinquants.

Ces délinquants sont plus rapides que nous. Peut-être qu'ils sont plus intelligents que nous dans le crime, et il faut changer de stratégie. Il faut regarder les choses de manière plus coordonnée.

Si nous adoptons une approche réductionniste et fragmentée, nous n'allons pas obtenir des résultats.

Peut-être que nous ne pourrons pas arrêter les délinquants complètement, mais on voit maintenant que cette délinquance augmente de manière exponentielle. Cela veut dire que les mesures en place doivent être réexaminées.

S'il vous plait, ne prenez pas ça comme une critique, il s'agit plutôt d'une mise en garde pour que l'on puisse voir ce problème d'un angle différent.

Certains disent que les plaintes n'ont pas été traitées parce qu'elles n'étaient pas complètes. C'est une question facile. Vous avez des outils de validation pour les plaintes, et donc toute

plainte qui est adressée à l'ICANN doit être validée. Si elle n'est pas validée, et qu'elle est incomplète, ce n'est pas une plainte.

Donc il faut éviter de recevoir quelque chose et de le considérer comme non traité.

Ensuite, je dirais qu'il faut voir si toutes les parties sont prêtes à faire quelque chose.

J'ai des doutes par rapport à cette volonté. J'ai vu plusieurs mesures, et des discussions qui ont commencé en 2007 par rapport à l'agenda de la cyber-sécurité. Et finalement, après beaucoup d'études et de travail, certains sujets ont été rejetés.

Je pense qu'on devrait voir s'il y a vraiment une volonté de toutes les parties d'un côté, ensuite essayer de préparer une stratégie à long terme, et trois : essayer de mettre en place des mesures qui puissent être coordonnées pour ne pas mettre en place des approches réductionnistes ou fragmentées.

Ce n'est pas un problème qui concerne une seule partie de la communauté, c'est un problème qui nous concerne tous.

MAGUY SERAD: Kavouss, j'aimerais rebondir sur ce que vous avez dit par rapport aux plaintes incomplètes. Ce que je voulais dire tout à l'heure c'était que quand nous recevons des plaintes de tiers, nous les

validons pour être sûrs que nous avons les informations correctes. Parce que parfois les gens n'apportent pas les informations complètes, ou pas de preuves concrètes. Et à ce moment-là, nous revenons vers la personne pour lui demander davantage d'informations.

Je voulais savoir qu'il ne s'agit pas … Que nous ne faisons que ne pas traiter cette plainte, nous faisons un suivi, nous revenons vers la personne qui a fait la plainte pour qu'elle nous adresse des informations supplémentaires.

Je voulais que vous sachiez comment le processus se met en place. Merci.

ALAN WOODS: Merci ; bonjour. Mon commentaire concerne le programme Beta dont vous avez parlé.

J'ai trois questions, cela peut être des questions où peut-être des réflexions.

Tout d'abord, qui sont les tierces parties dont on obtient des données ? Certains d'entre nous avons certaines exigences et chacun d'entre nous a des visions différentes par rapport à la liste noire de fournisseurs, en fonction de nos intérêts.

J'ai toujours posé la question, et je n'ai jamais reçu de réponse : est-ce que l'ICANN a une sélection de fournisseurs sur une liste noire ? Je voudrais savoir s'il y a des cas. Mais en même temps, nous devons être tout à fait clairs sur le fait qu'une liste noire de fournisseurs n'est pas quelque chose de concluant, parce que nous n'avons aucune sureté par rapport aux preuves. Et nous ne pouvons rien faire.

On ne peut pas dire : ce fournisseur il est sur une liste noire, donc on doit faire quelque chose. Il faut que l'on fasse des investigations ;

Quel est donc l'objectif de ce programme bêta et ensuite, est-ce qu'il y a, est-ce que vous pensez qu'il pourra y avoir une liste noire de meilleure qualité, entre guillemets, qui soit vérifiée par l'ICANN. Et comment est-ce qu'on va interagir avec les registres et les bureaux d'enregistrements.

CATHRIN BAUER-BULST: Merci beaucoup. On va donc recevoir la prochaine question, et ensuite on va répondre à ces deux questions. Qu'est-ce que vous en pensez ?

30 secondes ? 30 minutes ? Mais 30 secondes je pense que ce serait mieux, excusez-moi.

VOLKER GREIGMANN : Bonjour. Pour les parties contractantes, il est parfois difficile d'analyser les plaintes et de voir le tableau complet, parce que nous ne sommes pas des experts dans la gestion des noms de domaines et dans tous les autres domaines. Nous ne savons pas quelles sont les motivations juridiques, nous ne voyons pas le tableau complet.

Si on nous dit qu'il faut suspendre un nom de domaine, nous le faisons, et ensuite on nous dit il faut le remettre en place, mais nous ne savons pas vraiment quels sont les motivations ou les fondements. On nous dit…

On a une idée de ce qui peut se passer, mais on n'est jamais dédommagés en cas d'erreur.

Donc il est très difficile de prendre des décisions, parce que le risque économique repose sur nous toujours.

DAVID CONRAD: Pour répondre à Alan, l'origine de ce projet de recherche est un rapport qui a été publié où il y avait des statistiques sur l'abus du DNS. Et la méthodologie utilisée comme n'étant pas efficace. Il y avait une estimation du nombre d'abus dont faisaient l'objet les registres.

Donc le but de notre projet était de collecter des données d'autant de sources que possible. Nous n'avons pas de

limitations en nombre de sources. Et donc documenter une méthodologie publique que la communauté puisse consulter et sur laquelle on puisse se mettre d'accord.

L'intention était, le but était informatif. Nous aurons des informations, des données qui vont montrer quels sont les comportements au fil du temps.

L'ICANN, mon équipe, comme je l'ai dit avant, n'a aucune responsabilité en matière de conformité contractuelle, ce n'est pas notre travail, mais l'idée c'est de fournir des informations assez fiables à la communauté pour savoir quel est le niveau d'abus dont font l'objet les registres.

Pour que la communauté puisse utiliser ces informations et travailler pour améliorer les mesures d'atténuation d'abus du DNS.

Voilà, et je vais laisser Maguy répondre à la deuxième question.

CATHRIN BAUER-BULST: Je pense qu'on va clore cette séance parce qu'on n'a plus de temps. On sait que c'est une discussion très intéressante qui va continuer d'une manière ou d'une autre.

Et qu'est-ce qu'on en retient ? Il n'y a pas suffisamment d'informations, parfois il y a des informations qui rentrent en

conflit, on ne sait pas très bien quelle serait l'autorité de l'information. Et ce que je suggère : plus de coopérations entre le SSR et le département de conformité contractuelle. Certains des registres, certains TLD, font l'objet d'un plus grand nombre d'abus que d'autres. Et donc si nous ne pouvons pas nous mettre d'accord sur la validité des informations sur lesquelles nous basons nos conclusions, cela représente une difficulté. Il faudrait donc avoir une discussion par rapport à ce qui est considéré comme une information fiable.

Et le GAC et d'autres membres ont un rôle clef à jouer dans ces discussions.

Ensuite, je vais mettre l'accent sur la coopération. Car les différentes parties de la communauté sont surchargées par rapport au rôle qu'ils doivent avoir dans ce processus, donc il faut voir comment atténuer ces responsabilités.

Je vois que le mot atténuation est un mot clef de cette séance.

Je vais donc passer la parole à Bobby.

BOBBY FLAIM: Tout d'abord je tiens à remercier nos panélistes, Maguy, Dave, Craig qui a participé à distance et Greg. Merci à tous.

Je pense qu'on a eu d'excellentes présentations.

Je voulais ajouter à ce qu'à dit Cathrin, qu'il y a des questions encore concernant l'annexe 1. Il y a des informations basées sur cela, et je voulais mettre l'accent sur le rapport du CCRT qui est très utile.

Et en ce qui concerne ce que Keith et Kavouss ont dit, il faudrait donc adopter une approche plus systémique vis-à-vis des abus pour que les personnes, les délinquants, ne puissent pas utiliser le DNS.

Et ensuite, j'espère que nous allons pouvoir utiliser une partie des fonds de l'ICANN, et qui viennent des enchères, pour encourager ce type de mesures.

Merci à tous de votre participation, merci beaucoup d'avoir consacré votre temps à cette séance.

Merci beaucoup.

[FIN DE LA TRANSCRIPTION]