FR

ICANN82 | Forum de la communauté – ccNSO : séance du Comité permanent sur l'utilisation malveillante du DNS
Mercredi 12 mars 2025 – 13h15 à 14h30 PST

CLAUDIA RUIZ : Nous allons lancer l'enregistrement.

Bonjour et bienvenue à cette réunion de la ccNSO sur le comité permanent de l'utilisation malveillante du DNS. Je suis Claudia Ruiz, je suis la responsable de la participation pour cette séance avec ma collègue. Veuillez noter que cette séance est enregistrée et qu'elle est régie par les normes de conduite attendues de l'ICANN et la politique anti-harcèlement de la communauté de l'ICANN.

Au cours de cette séance, les questions et les commentaires soumis dans le chat seront lus à haute voix que s'ils sont formulés correctement comme indiqué dans le chat.

L'interprétation pour cette séance sera assurée en anglais, en espagnol et en français. Si vous souhaitez prendre la parole au cours de cette séance, levez la main dans Zoom. Lorsqu'ils seront appelés, les participants pourront activer leur micro dans Zoom et les participants sur place utiliseront un micro. Indiquez votre nom et la langue dans laquelle vous allez parler si vous parlez une autre langue que l'anglais et parlez à un rythme raisonnable pour permettre une interprétation précise.

Merci, et je donne la parole au président de cette séance, Nick Wenban-Smith.

NICK WENBAN-SMITH Merci Claudia.

Bienvenue à tous. C'est déjà une longue semaine et après le repas je sais que l'énergie est un peu en baisse, donc je vais essayer de rester intéressant pour présenter ce thème.

La méthodologie utilisée pour nos discussions a été faite de manière non scientifique à travers des enquêtes par le groupe de travail. Ce thème a été sélectionné. Nous avons eu un gagnant lors de notre réunion d'Istanbul. Et samedi, les deux thèmes qui étaient en première place pour le travail futur de notre communauté étaient l'intelligence artificielle et lutte contre l'utilisation malveillante du DNS. Mais c'est l'intelligence artificielle qui a gagné. Ce sont des thèmes tout à fait différents. Aujourd'hui, nous allons voir le crime, le délit sur l'Internet, les escroqueries, les enregistrements malveillants de nom de domaine, ce type de délits financiers.

D'abord, je vais vous présenter un peu ce que l'on va faire dans les prochaines réunions. Il y a plusieurs formats. On va travailler de manière plus informelle. Avant de commencer, je voudrais remercier le pays hôte, .us, et Fernando qui va nous faire un peu de promotion concernant les réunions de .us.

FERNANDO ESPANA : Bonjour à tous. J'espère qu'hier était bien, que vous vous êtes bien amusés lors de cet événement de réseautage. On a vraiment apprécié votre présence. Je sais que ces réunions après le repas sont un peu pénibles, donc vous avez de petits biscuits au fond de la salle. Servez-vous. Je sais que nous en sommes déjà à la cinquième journée de la réunion et je sais qu'on est fatigués. Mais de toute façon, je vous souhaite la bienvenue ici à Seattle. Je vous souhaite une bonne réunion.

NICK WENBAN-SMITH Merci beaucoup pour le registre GoDaddy de .us pour cette réception.

Ce thème intéressant concernant les données d'enregistrement, la collecte de ces données d'enregistrement et la vérification de ces données d'enregistrement permet de prévenir l'utilisation malveillante du DNS et de l'atténuer aussi. Nous avons deux présentations de deux ccTLD différents : nous avons Bob de .nz et Kristian de .se. Ils vont nous dire ce que font les ccTLD concernant les données d'enregistrement, la collecte et la vérification et l'impact que cela peut avoir sur la lutte contre l'utilisation malveillante du DNS. Puis, nous allons avoir une autre approche un peu plus approfondie concernant les termes de référence du comité permanent sur l'utilisation malveillante du DNS. Nous allons entendre mon ami Reg qui travaille pour Tucows qui est un bureau d'enregistrement mondial. Il a, je pense, une approche différente puisqu'il ne travaille pas seulement comme un ccTLD

individuel, il a différentes approches, il travaille avec différents ccTLD, avec des gTLD aussi, donc comment faire ce travail de manière globale. Et Chris Lewis-Evans va nous parler d'un point de vue du maintien de l'ordre puisqu'il travaille à l'agence de délit nationale de Grande-Bretagne.

Il y a une petite erreur là, aujourd'hui, on n'est pas mardi et il n'est pas 10 h 30. Je le précise.

Je vais d'abord donner la parole à mes collègues Bob et Kristian. On va essayer de faire quelque chose d'un peu informel. Je vais vous demander de prendre la parole, mais surtout d'essayer de présenter un peu ce que vous allez faire de manière intéressante pour que chacun ait envie de participer et qu'il y ait vraiment un dialogue. N'hésitez pas à vous porter volontaire pour prendre la parole.

Nous avons des diapositives. Ici, je rappelle aux participants ce que vous devez faire. Qui est là pour la première fois dans une réunion de l'ICANN ? Merci beaucoup et bienvenue. C'est un bon groupe, un bon endroit, un endroit dans lequel vous vous sentirez bien en sécurité. Bienvenue.

Les membres du comité permanent du DNS booth, vous pouvez vous lever s'il vous plaît pour montrer un peu qui vous êtes ? Fernando, Bruce, Olga, Chris, David, Bob ; merci à tous.

Nous ne sommes pas ici pour travailler dans le domaine de politique ; nous sommes ici pour partager de meilleures pratiques,

des informations, apprendre les uns des autres, connaître les erreurs aussi. Il s'agit ici d'un dialogue ; nous voudrions vraiment qu'il y ait un dialogue qui nous permette de lutter contre l'utilisation malveillante du DNS et tout cela dans l'ensemble de l'écosystème des ccTLD.

Nous comprenons qu'un ccTLD est un TLD et qu'on ne peut pas passer les abus de l'un à l'autre, on veut les éliminer. On souhaite qu'il y ait peu d'utilisations malveillantes dans la communauté de ccTLD et que ce soit la même chose dans l'écosystème des gTLD.

Ici, vous avez une liste de ressources avec une bibliothèque, une liste de contacts et d'adresses e-mail. Nous avons présenté des services, nous avons fait des enquêtes auprès des ccTLD en 2024, des enquêtes auprès aussi de ccTLD en 2022. Nous avons organisé des ateliers, nous avons présenté des outils, des mesures. Nous avons présenté des travaux sur les ressources des ccTLD et les utilisations malveillantes qui peuvent exister au niveau du DNS. Si tout cela vous intéresse, toutes ces ressources sont gratuites et sont à votre disposition et vous pouvez y accéder.

Nous parlons aussi de tout ce qui concerne les clauses contractuelles dans l'espace des gTLD réglementé par l'ICANN en termes d'obligations pour les registres et de bureaux d'enregistrement concernant l'utilisation malveillante du DNS et de l'adoption de ces différentes clauses.

Dans le contexte dans lequel nous travaillons qui est un peu le centre de notre travail, les données d'enregistrement, lors de

l'enquête DASC de 2024, on a constaté qu'il y avait beaucoup de pratiques différentes au niveau de la vérification des données d'enregistrement, y compris aucune pratique, une inexistence de pratique. Il y a certains bureaux d'enregistrement qui font beaucoup de vérification, d'autres qui n'en font aucune en fonction du modèle de registre que l'on a, en fonction du gestionnaire aussi, de la politique de ces registres. Rien n'est fait de manière automatique. On commence à faire ce type de chose lorsqu'on reçoit une plainte, des fois lors d'une rénovation, lors d'un transfert, lors de l'enregistrement, après l'enregistrement. Vous voyez qu'il y a toute une série de possibilités dans l'environnement dans lequel nous travaillons.

On va prendre un petit moment pour répondre aux questions du Menti. Je vous donne la possibilité de vous connecter au Menti. Est-ce que vous avez besoin d'un peu plus de temps ? Je vais me connecter pour avoir un peu avoir votre avis en général et connaître un peu votre opinion. Elle mesure si vous êtes d'accord ou pas avec cette déclaration, à savoir les données d'enregistrement doivent être exactes et cela est utile comme outil pour combattre l'utilisation malveillante du DNS. Vous pouvez répondre. 35 réponses. Je vois que les réponses entrent, 37, 38, 39, 40, 41. Vous voyez qu'on est à 8,4, 8,5, 8,2. Roelof, vous voulez poser une autre question ? Allez-y.

ROELOF MEIJER : Je pense que tout dépend comment vous lisez cette phrase, parce que les données exactes d'enregistrement sont bonnes pour prévenir l'utilisation malveillante, mais peut-être pas pour combattre ces utilisations malveillantes. D'abord, il faut être sûr que les données fournies par le titulaire sont des données exactes.

NICK WENBAN-SMITH : Oui, je comprends ce que vous voulez dire. Souvent, lorsqu'on fait ce type d'enquêtes Mentimeter, j'ai aussi cette sensation d'ambiguïté dans les questions.

Ici, certains ccTLD utilisent une plainte de délit concernant un nom de domaine. Ils vont utiliser la vérification des données du titulaire comme méthode pour retirer ce nom de domaine. C'est pour cela qu'on a posé cette question. Je crois que c'est une question intéressante. Le thème est un peu large, c'est pour cela que nous organisons cette séance. Les choses sont beaucoup plus compliquées qu'elles ne le paraissent.

NIGEL ROBERTS : Merci. Je suis d'accord avec ce que Roelof a dit. Nous sommes un de ces ccTLD que vous avez mentionnés justement. Je formulerai cela différemment. Je ne suis pas d'accord justement avec cette question. Les données d'enregistrement inexactes sont utiles comme outil pour combattre l'utilisation malveillante du DNS, parce que nous sommes contactés et la première chose que nous faisons, c'est de vérifier les données d'enregistrement, si ces

données d'enregistrement sont un peu bizarres. Nous lançons une vérification et si on ne peut pas vérifier ces données, nous allons suspendre directement sans aucune alternative.

NICK WENBAN-SMITH : Est-ce qu'il y a d'autres commentaires avant de passer aux présentations ? Très bien, alors nous allons passer aux présentations. Mais gardez vos commentaires parce que je pense que cela va être pertinent après les présentations. 8,1 sur 10, c'est un chiffre assez haut.

BARBARA PEARSE : Je suis de la Commission des noms de domaine de Nouvelle-Zélande. Je vais vous présenter comment nous gérons la validation des données, la vérification de l'identité dans le ccTLD .nz.

Pour vous donner un petit aperçu de notre rôle et de nos politiques, voici les critères d'éligibilité pour enregistrer un nom de domaine à .nz. Il faut avoir plus de 18 ans ou être une entité constituée légalement. Le .nz n'a pas de prérequis de présence locale. Parfois, il peut être difficile d'identifier des individus qui vivent dans d'autres juridictions.

Une autre méthode que nous utilisons est les données d'enregistrement qui doivent être exactes, complètes et à jour. Nous demandons beaucoup d'informations : le nom du titulaire de domaine, son adresse, sa ville, son code postal, le pays, le numéro de téléphone, l'e-mail ainsi que d'autres choses.

Et comme il l'a été dit précédemment, nous pouvons suspendre ou annuler un nom de domaine si les données sont inexactes ou si l'identité n'a pas pu être vérifiée en temps et en heure.

Nous avons deux méthodes pour faire cela. Nous avons établi un outil automatique pour pouvoir pointer les domaines qui pourraient utiliser de manière malveillante le DNS. Il y a une note qui est donnée par rapport aux noms de domaine sur les données qui ont été enregistrées. Nous allons d'abord vérifier manuellement les noms de domaine qui ont un mauvais score pour vérifier si les noms de domaine n'ont pas une note trop haute, par exemple si ce sont des volontés d'usurper l'identité de banques, d'agences de gouvernement, etc., dans ce cas-là, la note augmente. C'est un processus manuel où nous envoyons une requête au titulaire de domaine de répondre de confirmer les données d'enregistrement.

Une autre manière est un échantillon réactif où dans ce cas-là, des membres du public ou des agences nous réfèrent à des noms de domaine suspicieux. Dans ce cas-là, nous pouvons lancer une vérification des données également.

Lorsqu'il s'agit d'identification d'identité, nous avons une politique assez stricte qui s'applique sur plusieurs juridictions. Le titulaire de nom de domaine doit fournir une pièce d'identité avec photographie pour pouvoir passer ce test. Ce que nous voyons assez souvent, c'est la première étape, la validation des données ; si les données sont validées et que nous avons toujours

l'impression que le domaine est suspicieux, nous passerons par la phase de validation de vérification d'identité. Et souvent, ce qui fonctionne, c'est de demander des tests d'identité biométriques.

NICK WENBAN-SMITH : Est-ce que le nom de domaine reste disponible pendant ce temps-là ?

BARBARA PEARSE : Il reste dans la zone, effectivement ; donc, il n'y a pas de suspension tant que le processus de validation n'est pas complet.

Voici un exemple des étapes que nous avons rassemblées pour les trois premiers mois de notre échantillon. En ce qui concerne les chiffres, nous avons 226 noms de domaine qui n'avaient pas de données validées. Nous avons demandé une vérification de d'identité ; sept d'entre eux n'ont pas voulu vérifier leurs données. C'est une solution qui est assez prometteuse et qui pourrait être une solution à long terme pour nous.

Lorsque vous voyez ici l'échantillon réactif, les données qui n'ont pas été validées, nous en avons 51. Nous leur avons demandé de vérifier leur identité ; trois d'entre eux n'ont pas voulu. Nous les avons donc suspendus.

Pourquoi est-ce que l'échantillon réactif est plus bas que le proactif ? Parce qu'en général, nous avons des plaintes vis-à-vis de noms de domaine qui peuvent être des concurrents ou qui ont des

problèmes avec l'utilisation du nom de domaine ou le contenu. Il est donc normal que nous vérifiions cela.

NICK WENBAN-SMITH : Si j'ai bien compris, l'échantillon proactif, ce sont de nouveaux enregistrements et seulement trois d'entre eux étaient vérifiés. Donc, 99 % de l'échantillon proactif était une utilisation malveillante du DNS alors que dans l'échantillon réactif, nous voyons que ce n'est que 56 %.

BARBARA PEARSE : Oui, ils peuvent être compromis également.

REG LEVY : En ce qui s'agit de l'échantillon proactif, sur 226, vous en avez sept qui n'avaient de vérification. Et sur 97, trois n'ont pas été vérifiés. Alors, je ne comprends pas, au niveau des chiffres, il y a des chiffres qui ne correspondent pas.

BARBARA PEARSE : Oui, du côté proactif, c'est bon.

REG LEVY : Mais 54 plus 21, cela fait 72 noms de domaine.

NICK WENBAN-SMITH : J'avoue que le calcul mental n'est pas mon fort, mais 54+3+21, cela fait 97.

REG LEVY : Je me demande juste pourquoi on a perdu 20 noms de domaine.

BARBARA PEARSE : Je pense que c'est là un problème de calcul. Mais en général, il est important de noter que nous vérifions plus de noms de domaine grâce à la fonction réactive.

REG LEVY : Mais si on a ces domaines dans la colonne vérifiée, nous sommes presque à 50 %, mais vu qu'ils partent dans la colonne suspendue, nous sommes à 25 %.

BARBARA PEARSE : Nous avons moins de 1 % de tous nos noms de domaine qui sont soupçonnés d'utilisation malveillante du DNS. Prochaine diapo s'il vous plaît.

Nous voyons un vrai lien entre les données inexactes et l'utilisation malveillante du DNS. C'est donc un bon indicateur et la vérification est un outil pour nous au .nz. Les catégories que nous trouvons, ce sont d'abord des usurpations d'identité, tentatives d'hameçonnage et une utilisation frauduleuse et usurpation d'identité des gouvernements et des institutions financières. C'est ce que l'on voit en plus des noms de domaine compromis. Quand

ils sont compromis, il est utile d'avoir des données mises à jour puisque dans ce cas-là nous pouvons contacter les titulaires de nom de domaine et nous pouvons aider ceux-ci à résoudre les problèmes.

C'est tout ce que j'avais à présenter. Est-ce qu'il y a des questions ?

NICK WENBAN-SMITH : Oui, je crois que nous avons beaucoup de questions, surtout sur le point politique de vos positions. Vous dites que c'est moins de 1 % et que le processus de vérification est un effort à faire pour l'opérateur de registre. Ce n'est pas très pratique au niveau de l'expérience de l'utilisation, surtout si on est titulaire de nom de domaine. Comment est-ce qu'on trouve l'équilibre entre la sécurité du TLD et l'expérience d'utilisation ? Est-ce qu'on va trop loin pour finalement 1 % de noms de domaine frauduleux alors que la majorité sont des titulaires légitimes ?

BARBARA PEARSE : Nous avons une approche basée sur les risques et c'est pour cela que nous utilisons des échantillons et nous donnons une note de probabilité d'utilisation malveillante du DNS.

KRISTIAN ØRMEN : Je suis Kristian Ørmen et je suis de la fondation suédoise sur l'Internet et nous avons les .nu et .se.

Quelques statistiques. Nous avons 105 titulaires de nom de domaine. Nous avons des prérequis très stricts et les opérateurs de registre doivent vérifier les titulaires de nom de domaine. Mais nous sommes assez raisonnables sur ces questions.

Nous avons près de 1,5 million de noms de domaine sur le .se et nous avons une échelle de prix différente. C'est pour cela que j'ai donné ici les chiffres moyens. Si nous avons des prix différents, c'est parce que nous donnons une réduction aux opérateurs de registre qui vérifient les données avant l'enregistrement.

La première question, c'est : est-ce que la vérification des titulaires est une solution pour la réduction de l'utilisation malveillante du DNS ? Non. Oui, c'est utile, mais peu importe le nombre de vérifications que nous faisons, cela ne résoudra pas le problème de l'utilisation malveillante du DNS, puisque les malfaiteurs deviendront meilleurs et nous ne pouvons pas faire comme les banques, vérifier les identités de tous nos consommateurs et les connaître de manière personnelle. Mais nous devons être raisonnables et nous devons s'attaquer à l'utilisation malveillante du DNS quand elle est présente. Nous devons faire face à cette utilisation malveillante.

Comme je l'ai dit sur ma diapo, il est évidemment utile pour la police d'avoir les informations lorsqu'elles arrivent. Je n'aime pas vraiment lorsqu'ils nous contactent et qu'on leur dit que nous n'avons pas d'informations à leur donner, ce n'est pas forcément agréable. Mais d'un autre côté, l'alternative est de dire : « Ce

titulaire est sous l'entreprise AB, mais parfois, ce type de données n'est pas suffisant. » Évidemment, quand on s'attaque à des sites Web qui viennent d'arriver, il est toujours plus utile de pouvoir contacter le titulaire de nom de domaine.

Autre chose de très important dans mon registre, nous voulons corriger les données des domaines parce que nous voulons être capables de vérifier un titulaire de nom de domaine lorsqu'il nous dit : « J'ai perdu mon domaine et ce bureau d'enregistrement ne veut pas m'aider » ; alors on regarde et on va leur dire par exemple : « Ce n'est pas votre domaine. » Si votre nom est Anders Andersen, cela doit figurer comme cela dans vos données d'enregistrement. C'est très important que les données du titulaire de nom de domaine soient correctes.

Comme je l'ai dit, nous sommes raisonnables concernant les exigences. En général, lorsqu'un bureau d'enregistrement me demande ce qu'il doit vérifier, dans quelle mesure il doit vérifier l'exactitude de données, je leur dis d'essayer de ne pas utiliser des données mensongères. Si vous êtes un bureau d'enregistrement en Suède, vous avez beaucoup de clients suédois, vous pouvez vérifier la compagnie pour voir si le nom est correct, ce type de vérification. Ensuite, vous pouvez demander aux personnes de se connecter, mais c'est un peu trop. Donc, on n'a pas ce type d'exigence.

Nous avons mis en œuvre un nouveau système qui demande quand même un peu plus de choses. Pour les nouveaux domaines, nous utilisons l'identité électronique, nous faisons une vérification

prédélégation, nous regardons l'enregistrement. S'il y a quelque chose qui ne marche pas, nous allons rentrer dans le domaine, voir le serveur, nous allons demander au bureau d'enregistrement de revérifier le titulaire. Et en général, on fait une vérification approfondie du titulaire.

On a conçu ce système comme cela parce que ce qui nous paraît le plus important, c'est de pouvoir augmenter le niveau de contrôle ultérieurement si nécessaire, et s'il y a une erreur, on doit revérifier le titulaire. Nos vérifications peuvent être approfondies si nécessaire. Nous avons un premier niveau, mais nous pouvons aussi voir grâce à l'intelligence artificielle par exemple si c'est un domaine malveillant.

Actuellement, nous avons appliqué ce nouveau système. Je pense que nous avons une centaine de domaines actuellement que nous avons vérifiés de cette manière. Nous avons quelques vérifications que nous n'avons pas encore faites. Mais les bureaux d'enregistrement doivent s'habituer à ce nouveau système. C'est pour cela que nous allons doucement.

NICK WENBAN-SMITH : Quand avez-vous commencé à utiliser ce système d'ID électronique ?

KRISTIAN ØRMEN : Nous avons commencé le 1er janvier 2023. Et maintenant, nous avons les deux plus grands bureaux d'enregistrement qui

l'utilisent. Et 40 % des nouveaux enregistrements se font en validant cette identité électronique. Cela coûte 25 couronnes, environ 2,5 $, et cela paie les coûts du système qu'on utilise. Pour certains bureaux d'enregistrement, c'est très intéressant parce qu'ils vont économiser de l'argent sur leurs enregistrements.

NICK WENBAN-SMITH : Il y a plusieurs questions, Luc, Bruce et peut-être Reg. Luc, allez-y.

LUC SEUFER : Une question à Barbara. Peut-être que je vois un peu trop les possibilités de conspirer partout, mais j'aimerais bien savoir ce que vous voulez dire quand vous parlez d'un vol de nom de domaine. À ce moment-là, on pourrait avoir un problème d'hameçonnage s'il s'agit d'un magasin de contrefaçon. On a différents types de problèmes.

BARBARA PEARSE : C'est le vol d'une marque. Quand on connaît les marques qui ont un nom de domaine, on va utiliser ce nom pour qu'il apparaisse sur le site Internet de l'organisation en se faisant passer pour la marque. C'est une espèce d'hameçonnage, mais il faut le déterminer. On a un processus de validation de données qui doit être mis en place.

LUC SEUFER : Donc, ce n'est pas une utilisation malveillante du DNS selon la définition de l'ICANN.

BRUCE TONKIN : Une autre définition de faux magasin, c'est quand cela a l'air d'être un magasin, on a des services proposés et la personne va utiliser sa carte de crédit, va acheter quelque chose, l'argent va être retiré, mais c'est une escroquerie. C'est un magasin, ce n'est pas une marque en particulier.

NICK WENBAN-SMITH : Nous avons parlé de cela, on a parlé de la définition de certains termes, d'utilisation malveillante, d'hameçonnage. Cela nous a demandé du temps, il a fallu définir chaque terme, qu'est-ce qui correspondait à l'hameçonnage, au délit financier, au vol de propriété intellectuelle, ce type de choses. De toute façon, ce sont des activités délictuelles et la plupart des ccTLD seront pénalisés. Il y a des politiques et de processus en place pour retirer ces TLD. C'est intéressant de toute façon de voir ici un faux magasin qui fait de l'hameçonnage.

BRUCE TONKIN : Kristian, vous avez parlé d'eID. Comment faites-vous pour faire payer ?

KRISTIAN ØRMEN : Il y a plusieurs solutions d'eID. Nous proposons aux bureaux d'enregistrement de choisir la solution qu'ils préfèrent. Il y a quelques petites exigences standards. En Suède, il y a ce qu'on appelle un ID bancaire pour ce type de petites transactions et on peut payer comme cela. S'il y a des titulaires qui viennent d'autres pays, cela peut ne pas fonctionner, donc ils peuvent utiliser un autre système.

NICK WENBAN-SMITH : Est-ce que c'est clair au niveau du registre et du système d'enregistrement, de recherche de registre comme le RDAP ? Qui va vérifier les domaines ?

KRISTIAN ØRMEN : En général, nous n'utilisons pas le WHOIS. Nous utilisons seulement un encouragement à présenter tout cela.

CHRIS LEWIS-EVANS : Vous avez mis deux ans ? Vous avez des données du niveau de l'utilisation malveillante enregistrées en fonction des mécanismes utilisés à partir de l'utilisation d'eID ?

KRISTIAN ØRMEN : L'année dernière, nous étions à 20 % de volume et maintenant, nous en sommes à 40 % de volume d'utilisation avec l'eID. Je dirais que cela augmente et que la plupart des utilisations malveillantes que nous constatons viennent de bureaux d'enregistrement qui

n'utilisent pas cet encouragement à utiliser l'eID. Il faut faire une recherche là-dessus.

NICK WENBAN-SMITH : Et qu'est-ce que vous faites pour essayer de convaincre les bureaux d'enregistrement d'utiliser cela ? Quel est l'encouragement que vous utilisez ? La partie financière ?

KRISTIAN ØRMEN : Pour l'eID, nous les encourageons à utiliser le système. Quand il s'agit de l'utilisation malveillante, nous en parlons, nous essayons d'encourager les bureaux d'enregistrement à vérifier les données de leurs clients. Nous pouvons regarder la prochaine diapositive si vous voulez parce que j'ai mis ces chiffres dans cette diapositive.

Nous avons indiqué une exigence dans nos contrats pour les bureaux d'enregistrement. S'ils ont des données incorrectes de leur clientèle, ils doivent désactiver le domaine. C'est un gros problème pour un bureau d'enregistrement parce que cela veut dire qu'il y a beaucoup d'anciens domaines avec des données incorrectes d'enregistrement, donc ils ne veulent pas le faire. Et on voit des domaines qui ont donné lieu à des utilisations malveillantes. En général, cela correspond à des données incorrectes. Et les bureaux d'enregistrement le savent.

REG LEVY : À propos de l'eID, apparemment, c'est facile de vérifier les données concernant une personne en Suède. Mais ce n'est pas la même

chose au Royaume-Uni par exemple. Est-ce qu'un bureau d'enregistrement peut avoir un prix préférentiel pour les domaines qui fournissent une vérification eID par exemple ?

KRISTIAN ØRMEN : Oui, cela se fait par domaine. Nous avons un système : le bureau d'enregistrement doit montrer s'il utilise l'eiD ou pas et il y a une question dans le guide qui dit si c'est un bureau d'enregistrement qui l'utilise, on va voir quelle est la documentation utilisée et on va faire une vérification de cet eID.

PIERRE BONIS : Merci pour cette présentation. Je voudrais savoir, lorsque vous vérifiez un nouveau nom de domaine, lorsque vous décidez que vous n'allez pas l'activer pour une raison X, est-ce que vous faites quand même payer le bureau d'enregistrement ?

KRISTIAN ØRMEN : Oui, le domaine sera enregistré, il y aura une erreur de la part du bureau d'enregistrement, on demandera de revérifier et le domaine sera dans le registre jusqu'à la date d'expiration. S'il ne vérifie ces données pendant un an, cela restera là, même pendant 10 ans. Nous ne voyons aucune raison de l'effacer. Nous demandons au bureau d'enregistrement de s'en occuper, de voir s'il peut régler le problème et si ce n'est pas le cas, le nom restera là.

PIERRE BONIS : Et si le bureau d'enregistrement décide d'effacer ce nom de domaine parce qu'il se rend compte que les données sont incorrectes, est-ce que vous allez faire payer le bureau d'enregistrement ou est-ce que vous lui donnez une période de grâce ?

KRISTIAN ØRMEN : Nous avons une liste de tous les enregistrements. Nous allons avoir un calendrier avec les enregistrements qui ont eu lieu de certains domaines et ensuite, nous allons voir les incidents. Nous allons voir comment on peut prévenir ce type d'incident dans le futur. En général, on ne fait pas payer un nom de domaine qui a été enregistré et qui pose problème par la suite.

ROELOF MEIJER : Est-ce que vous avez des résultats concernant l'impact de ces chiffres sur les noms de domaine enregistrés de manière malveillante ?

KRISTIAN ØRMEN : Non, nous n'avons pas ces chiffres. Je peux effectuer des recherches, mais je dirais que c'est quelque chose qui se fait de manière volontaire. Si vous voulez utiliser de manière malveillante un domaine de .se, vous allez choisir de vous enregistrer dans eID parce que sinon, vous risquez d'être plus facilement détecté. Donc,

on constate que si on a un bon système d'enregistrement, les choses sont plus faciles à contrôler.

NICK WENBAN-SMITH : C'est une initiative qui est connectée à l'obligation de NIS2 ?

KRISTIAN ØRMEN : Oui et non, parce que c'est quelque chose que nous avons lancé il y a plus longtemps que cela. Nous savions dès le début que NIS2 allait être mise en œuvre, donc il fallait qu'on s'y adapte. Mais nous ne savions pas quel serait le champ d'application exact de NIS2 ou quel serait le texte exact. Nous voulions utiliser cela comme encouragement. Nous voulions montrer que cela fonctionnait et nous voulions également que les bureaux d'enregistrement fassent des vérifications et de montrer aux autres que c'était possible. S'il y a des exigences de la part de l'Union européenne, nous pouvions déjà montrer que cela fonctionnait et que comme cela fonctionnait déjà au niveau des bureaux d'enregistrement, nous n'avons pas besoin de nous référer aux opérateurs de registre, parce que les bureaux d'enregistrement font partie de l'écosystème.

NICK WENBAN-SMITH : Et en Suède, il y a ce système d'identité en ligne.

KRISTIAN ØRMEN : Oui. Presque tout le monde en a sauf moi d'ailleurs. Si on me demandait ma pièce d'identité en ligne, je ne pourrais pas.

NICK WENBAN-SMITH : Au Royaume-Uni, nous avons une carte d'identité, mais nous n'avons pas encore de carte d'identité numérique.

KRISTIAN ØRMEN : Je sais que j'avais peut-être trop inscrit sur mes diapositives, mais voulais quand même finir là-dessus parce que le 1er mai, nous allons lancer un nouveau système qui nous permettra de mieux travailler avec de gros volumes. Ce que l'on pourra faire, c'est que si l'on trouve un domaine où il y a des données étranges, nous pouvons mettre tout le domaine dans le système. Le bureau d'enregistrement recevra un message pour vérifier tout le domaine. On laisse en général 60 jours pour vérifier les données. Par exemple, nous avons 12 000 domaines où nous avons vu que dans le bureau d'enregistrement l'entreprise n'existait pas, donc nous avons mis cela. Et si nous voyons que c'est utilisé pour utiliser le DNS de manière malveillante, nous faisons un cas par cas, évidemment, mais nous pouvons être flexibles. Et nous essayons de suivre le même chemin que possible.

Je crois que c'était ma dernière diapo, oui.

NICK WENBAN-SMITH : Merci, c'était très intéressant.

J'avais une question pour Reg. Est-ce que vous êtes un bureau d'enregistrement ?

REG LEVY : Oui.

NICK WENBAN-SMITH : Alors, comment est-ce que vous gérez avec toutes ces règles ccTLD et les gTLD avec des règles ? Est-ce que vous aimez cet encouragement financier ?

REG LEVY : J'ai une équipe qui s'occupe de la conformité, ils sont 10, et ils s'occupent de la conformité pour les gTLD, parce qu'il y a tellement de ccTLD que nous gérons que nous avons une autre équipe pour les ccTLD et pour vérifier la conformité pour les ccTLD. L'utilisation malveillante du DNS, c'est nous qui nous en chargeons, mais si nous avons besoin de suspendre ou de prendre en note des actions, dans ce cas-là, c'est nous qui nous en occupons. Mais c'est toujours très confus.

NICK WENBAN-SMITH : Oui, je me demandais quels étaient les défis d'avoir différentes échelles entre les ccTLD et les gTLD, différentes règles. Est-ce que cela pourrait expliquer les différences de régime de conformité, par exemple si on est au Danemark ou en Suède, on peut avoir différents régimes. C'est pour cela que ma question était liée au nombre d'enregistrements dans les gTLD qui sont légitimes. Et c'est un coût, c'est un inconvénient qui se retrouve pour tous.

REG LEVY : Nous voyons que la plupart des enregistrements sont valides et les données d'enregistrement sont légitimes. Mais nous n'avons pas fait l'expérience d'être ciblés parce que nous avons énormément de TLD. La plupart des personnes ne savent même pas que nous existons puisque nous sommes un bureau d'enregistrement et nos clients .se sont des détaillants et les clients pour le .de sont des détaillants allemands. Il y a des exceptions, bien sûr, mais nous ne sommes pas ciblés par des utilisations malveillantes du DNS.

NICK WENBAN-SMITH : Quel est votre point de vue ? Est-ce que vous pensez qu'il est utile de vérifier les données d'enregistrement, soit pour empêcher les enregistrements malicieux, soit pour répondre aux plaintes d'hameçonnage, les rapports qui ont besoin de processus de vérification pour pouvoir enlever les noms de domaine du DNS si besoin ? Est-ce que vous êtes au-dessus de la moyenne ou en dessous de la moyenne du 8,2 ou est-ce que c'est vraiment juste un problème pour vous ?

REG LEVY : J'étais en dessous de 8,2 parce que je ne vois pas de lien de cause à effet entre les données lors de l'enregistrement et l'utilisation malveillante du DNS. Cela peut être vu également et je peux prendre par exemple le .edu. Il est très difficile d'avoir un domaine sous le .edu. Il faut être une entité. Et il y a énormément

d'utilisation malveillante du DNS avec ce .edu. Pourtant, pour pouvoir demander ce .edu, on ne peut pas être une simple personne parce que ces .edu ouvrent leur accès aux étudiants, ils ont des domaines, des sous-domaines, des URL, etc.

Donc, il n'y a pas toujours une relation entre les données soi-disant exactes et l'utilisation malveillante du DNS. Et je dis soi-disant parce que l'exactitude est déterminée de manière différente en fonction des personnes. Kristian nous présente une identification en ligne, Barb nous présentait des données biométriques et ce sont deux manières différentes de mesurer l'exactitude. Chaque TLD détermine ce qui est exact d'une manière différente. Lorsque l'on dit : « Est-ce que l'exactitude des données est utile pour lutter contre l'utilisation malveillante du DNS ? », déjà, je ne sais pas ce qu'est l'exactitude parce que nous n'avons pas tous la même définition, et ensuite, je ne vois pas de lien entre l'exactitude des données et la présence d'utilisation malveillante du DNS.

NICK WENBAN-SMITH : C'est très intéressant parce que la plupart d'entre nous dans la salle avons mis beaucoup de temps à nous assurer que les données soient exactes, même en tant qu'opérateurs de registre. Le fait d'avoir des données exactes est un point fondamental.

KRISTIAN ØRMEN : Un point à dire. Nous avons bien plus de données inexactes que d'utilisations malveillantes du DNS, donc on ne peut pas dire que

l'un est égal à l'autre. Ce sont deux choses complètement différentes.

NICK WENBAN-SMITH : Tout à fait. Les ccTLD, y compris le .uk, se plaignent de tentatives d'hameçonnage par exemple et la première chose que nous faisons est de vérifier les données d'enregistrement pour essayer de résoudre le problème très rapidement. Et si ces données sont inexactes, cela nous donne un indice sur le pourquoi du comment.

CHRIS LEWIS-EVANS : Je vais revenir au début. La question qu'on nous a posée, c'est est-ce que l'exactitude des données est utile pour combattre l'utilisation malveillante du DNS ? Qu'est-ce que combattre ? Kristian a dit que les données ne sont pas liées. Pour moi, combattre l'utilisation malveillante du DNS, c'est d'enlever l'utilisation malveillante du DNS de l'écosystème en ligne. Comment on fait ? On peut suspendre un domaine pour protéger les utilisateurs. Vous pouvez aider la police également pour suspendre ce domaine. Nous protégeons les utilisateurs, la police combat le malfaiteur. Mais la plupart du temps, dans les ccTLD, nous avons l'enregistrement au niveau des noms de domaine et ce que nous voyons au niveau des cc, c'est qu'il y a plus de noms de domaine qui ont plus de sept ans, voire plus. Ce sont des domaines qui sont compromis. Nous ne voulons pas les suspendre, mais pour combattre l'utilisation malveillante du domaine, on peut arrêter la personne responsable de ce domaine qui est piraté, mais cela ne

nous aidera pas. Ce qui nous aidera, c'est d'aider la personne dont le domaine a été piraté, de récupérer son domaine. Et on a besoin de données exactes pour pouvoir les contacter. Comment la police peut aider cette personne si nous n'avons pas les données de contact ? Souvent, ce qui se passe, quand les domaines sont piratés, c'est parce que les titulaires sont également les hôtes, ils ne mettent à jour leurs données et il est donc difficile pour nous de les contacter. Il faut absolument que les données soient exactes pour nous permettre de combattre le piratage et l'utilisation malveillante du DNS. Je pense que c'est pourquoi l'exactitude des données est utile et je recommande aux cc de continuer à le faire. D'un autre côté, cela crée un obstacle ou un point de conflit pour les enregistrements. Les criminels sont paresseux. Ils se dirigeront vers du crime qui est facile, pas cher et qui touchera le plus de monde possible. Si tout le monde avait ces obligations d'enregistrement, ils seraient toujours là, ils veulent gagner de l'argent. C'est leur gagne-pain.

Est-ce que c'est le remède unique pour combattre toute l'utilisation malveillante du DNS ? Non, l'utilisation malveillante continuera d'exister. Cela créera de la friction. Mais je crois que l'exactitude des données aide à lutter contre le cybercrime pour pouvoir aider à contacter les victimes de ce type de crime.

NICK WENBAN-SMITH : D'accord. Reg et Bruce.

REG LEVY : Nous nous concentrons sur la possibilité de contacter nos clients, parce que pour nous, tant qu'on peut contacter nos clients, cela nous permet d'atténuer l'utilisation malveillante et ses conséquences. Si par exemple j'ai 11 adresses e-mail, comment on sait que tout est exact ? Du moment qu'on puisse me contacter, c'est le principal. Mais mon vrai problème, c'est les licences d'utilisation d'Internet. On ne demande pas d'identification lorsqu'on achète du papier et des timbres, mais à certains endroits, nous avons commencé à demander une pièce d'identité pour exister en ligne. Ce n'est pas que pour les ccTLD, mais sur certains réseaux sociaux par exemple, on commence à demander une pièce d'identité ; c'est un problème, c'est une source d'inquiétude pour moi.

NICK WENBAN-SMITH : Est-ce qu'il y a des questions, que ce soit en ligne ou sur place ?

BRUCE TONKIN : Un point sur les nouveaux enregistrements. Sur les données d'enregistrement qui viennent d'arriver il y a un mois par exemple ou si ce sont des données qui sont dans le système depuis plus de sept ans par exemple, ils sont accueillis sur des solutions de gestion. Et dans ces cas-là, les données d'enregistrement ne sont plus adaptées plutôt qu'inexactes. Ce que les opérateurs de registre et les bureaux d'enregistrement font, c'est qu'ils essayent

de renouveler les domaines, mais le renouvellement n'est qu'un renouvellement de moyen de paiement et pas de vérification des données.

NICK WENBAN-SMITH : Donc on peut lutter contre l'activité délictuelle, lutter contre par exemple le blanchiment d'argent. On sait que le fait que les banques et des institutions qui travaillent bien n'empêche pas que le blanchiment d'argent ait lieu. Ce n'est pas toujours la solution. Kristian, allez-y.

KRISTIAN ØRMEN : Pour reprendre un peu ce qui a été dit concernant la capacité à contacter notre clientèle, ces outils, à l'origine, nous avions le groupe de coopération avec NIS2 qui nous a donné certaines recommandations, et j'ai constaté dans leur document qu'ils recommandent un e-mail, un numéro de téléphone. Et il y a certaines définitions, ils disent par exemple que pour les noms de domaine de risque moyen ou élevé, nous recommandons de vérifier le nom du titulaire de nom de domaine. On dit qu'il faut vérifier le numéro de téléphone et l'adresse e-mail et dans certains cas faire davantage de vérifications. Je ne suis pas un avocat, mais je trouve que c'est intéressant de voir qu'il y a moins d'exigences que ce que je pensais à l'origine. La capacité à contacter notre clientèle est très importante.

NICK WENBAN-SMITH : Mon expérience en tant qu'avocat est que si on a beaucoup d'utilisations malveillantes, cela veut dire qu'il y a quelque chose qui ne va pas, il faut augmenter la vérification, avoir un ccTLD bien organisé dans ce sens, c'est important. Et c'est une bonne défense pour les citoyens et la communauté en général.

Pierre, allez-y.

PIERRE BONIS : Je voudrais reprendre deux points. L'importance de la capacité à contacter notre clientèle, quand on parle de noms de domaine malveillants, la capacité de joindre le titulaire de nom de domaine pour ce faire, il faut avoir un nom. Et parfois, c'est beaucoup plus facile pour un registre de s'assurer que le titulaire va répondre que de voir si le titulaire est vraiment la personne qu'il prétend être.

Deuxième point, je suis d'accord avec ce que Kristian vient de dire, à savoir que quand on utilise le système de vérification de données pour lutter contre l'utilisation malveillante du DNS, puisque c'est notre premier outil, 99 % des vérifications que nous lançons quand on sait qu'il y a une utilisation malveillante qui est en jeu nous montrent que les données ne sont pas correctes. Et en général, la plupart des données non mises à jour ou non exactes ne mènent pas obligatoirement à des utilisations malveillantes du DNS. L'équivalent entre données exactes et utilisations malveillantes, je dirais que cette connexion n'est pas toujours convaincante.

NICK WENBAN-SMITH : Lorsqu'AFNIC contacte le titulaire, est-ce que le titulaire sait qui est AFNIC ? Comment le persuadez-vous que vous êtes une personne honnête, que vous êtes AFNIC ?

PIERRE BONIS : C'est une bonne question. Très souvent, les titulaires nous disent qu'ils ne savent pas qui on est, qu'on est peut-être un escroc. Donc, on envoie cette requête en même temps au bureau d'enregistrement et au titulaire de façon à ce que si le titulaire ne nous fait pas confiance, qu'il ait confiance en son bureau d'enregistrement qui va confirmer notre identité.

NICK WENBAN-SMITH : Peut-être. Mais parfois, le bureau d'enregistrement sur les enregistrements du registre n'est pas la même personne que le titulaire a contactée pour avoir son nom de domaine. Parfois, c'est un revendeur.

PIERRE BONIS : C'est pour cela que c'est bien d'envoyer à deux reprises ce type de requête. On envoie une première requête et s'il n'y a pas de réponse, au bout de 30 jours nous effaçons ce nom de domaine, parce que peut-être que le titulaire [inaudible] cela à un revendeur, à un bureau d'enregistrement. En tout cas, ce qu'on sait, c'est que

le nom de domaine ne fonctionne pas. Si vous êtes une personne honnête, vous allez tout de suite réagir.

NICK WENBAN-SMITH : Les données d'enregistrement sont utilisées comme outil pour combattre l'utilisation malveillante du DNS, mais si vous êtes un état étranger et un acteur d'un état étranger, vous voulez faire des actions malveillantes et ce type de vérification, vont-elles pouvoir tout de suite se rendre compte de l'identité de ce délinquant ?

KRISTIAN ØRMEN : Une réponse rapide. Nous utilisons ces vérifications, nous les faisons avec des bureaux d'enregistrement. Nous devons toujours nous rappeler que nous devons aussi vérifier le titulaire. Nous lui donnons un délai de 24 heures. Parfois, c'est trop peu, donc il faut que ce soit un délai raisonnable. Nous devons voir la gravité de la situation et en fonction de cela, nous allons donner un délai plus ou moins long. En tout cas, le délai doit être raisonnable pour que la personne puisse fournir des preuves de façon à ce qu'on ne passe pas à une suspension tout de suite si cette personne répond. Donc, il ne faut pas avoir trop de pouvoir, nous ne sommes pas la police, nous devons créer des [inaudible] types qui vont nous aider à travailler sur ces noms de domaine sur Internet et à faire certaines actions. Mais la police reste la police.

NICK WENBAN-SMITH : Luc, allez-y rapidement.

LUC SEUFER : Donc, quand on a des données incorrectes, je suis d'accord avec Kristian, mais pas toujours. Les délinquants ne sont pas toujours paresseux. Par exemple, nous revendons .cu de Cuba, c'est un domaine qui requiert une présence locale et nous le revendons. Nous avons en général un revenu de plus de 1 200 $ par an. Et de toute façon, il y a encore de temps en temps des utilisations malveillantes constatées.

IRINA DANELIA : Je suis de .ru. Nous parlons d'enregistrements de deuxième niveau ; c'est important. Prenons un exemple.

Admettons que nous voulons vérifier des données pour suspendre un nom de domaine et ce que nous voyons, c'est que beaucoup d'utilisations malveillantes du DNS se font d'un nom de domaine du troisième ou du même cinquième niveau. Je voudrais savoir quoi faire dans cette situation. Est-ce qu'on peut considérer qu'il va y avoir une manière de punir le titulaire de nom de domaine de deuxième niveau ? Comment faire dans ces cas-là ?

REG LEVY : Je vais vous répondre. Je ne vais vous regarder, mais je vais vous répondre.

Nous allons regarder le titulaire du nom de domaine de deuxième niveau parce qu'en général, ces troisième, quatrième et cinquième niveaux sont liés. Ce sont des domaines enregistrés de manière

malveillante et nous allons pouvoir les suspendre. Ou cela veut dire que le domaine de deuxième niveau a été victime d'une utilisation malveillante du DNS et que la personne va avoir accès au deuxième niveau et au reste des niveaux. Quand j'utilise le terme deuxième niveau, cela veut dire que le domaine de troisième niveau est .co.uk, parce que nous sommes en train de vendre .co.uk.

NICK WENBAN-SMITH : Merci. Kristian, est-ce que vous voulez ajouter quelque chose ? Nous allons répéter la question très rapidement et nous allons refaire une enquête ensuite.

KRISTIAN ØRMEN : Nous avons un acteur qui vend des domaines de sous-niveau sur .com.se et nous avons beaucoup de rapports d'utilisation malveillante. Si on veut fermer .com.se, il va falloir fermer beaucoup d'autres sites qui travaillent en Suède et qui pourraient être des domaines de sous-niveau de .com.se qui sont problématiques, mais il y a aussi de bons domaines. On ne peut pas suspendre tout le monde.

CHRIS LEWIS-EVANS : Rapidement, à propos d'AFNIC, si vous envoyez un e-mail à quelqu'un, vous ne savez pas qui il est ou vous ne savez pas exactement qui il est, vous avez plusieurs moyens de le contacter. Si l'adresse e-mail n'est pas correcte, vous ne pouvez pas garantir la capacité de le contacter. Donc, avoir des données exactes dans

votre point de contact est très important et cela ne veut pas dire d'avoir qu'une adresse e-mail, parce que si vous voulez contacter ces personnes, vous ne pourrez pas les contacter et vous allez devoir suspendre leurs domaines.

NICK WENBAN-SMITH : Parfois, je vois que le contact e-mail du titulaire est le même que celui que je suis sur le point de suspendre, et c'est un gros problème.

On passe à notre enquête de Mentimeter. Les données d'enregistrement exactes sont utiles en tant qu'outil pour combattre l'utilisation malveillante du DNS, c'est la question. Nous voyons les chiffres qui augmentent. On a 41 participants. C'est intéressant. Ce n'est pas nécessairement ce que je pensais obtenir. On a eu une longue discussion entre experts sur l'importance des données d'enregistrement et finalement, le résultat est que c'est moins important que ce ne l'était au début de notre séance.

KRISTIAN ØRMEN : On se rend compte que les données d'enregistrement sont très importantes, mais que cela ne va pas permettre de régler tous les problèmes d'utilisation malveillante du DNS. Je crois que c'est important d'en tenir compte.

NICK WENBAN-SMITH : C'est un peu plus bas. Commentaire final, un de mes livres préférés est justement sur les preuves médicales qu'on peut avoir dans

certains problèmes de tests cliniques. En fonction de l'écosystème, on peut avoir différentes règles, différents endroits géographiques aussi, différents acteurs, la confiance qu'on peut avoir dans le public, la facilité de tromper les gens ; tout cela est important. Ce sont des points dont il faut tenir compte.

Nous sommes arrivés à la fin de notre séance. Je vous remercie. C'était une séance très intéressante. Si quelqu'un veut venir me voir, venez. Il va y avoir aussi d'autres séances. Il va y avoir des séances pour les nouveaux arrivants. Je remercie les intervenants. Et la séance est maintenant terminée. Merci.

[FIN DE LA TRANSCRIPTION]