ICANN83 | Forum de politiques – Discussion du GAC sur l'atténuation de l'utilisation malveillante du DNS
Mardi 10 juin 2025 – 09h00 à 10h15 CEST

JULIA CHARVOLEN

Bonjour et bienvenue à cette séance du GAC sur l'utilisation malveillante du DNS, ce mardi 10 juin à 7 h UTC, Veuillez noter que cette session est enregistrée et qu'elle est régie par les normes de comportement attendues de l'ICANN et par la politique anti-harcèlement de la communauté l'ICANN. Les questions ou commentaires seront lus à haute voix uniquement s'ils sont présentés suivant le format approprié et soumis dans le chat de Zoom. L'interprétation de session se fera dans les six langues de l'ONU plus portugais.

Si vous souhaitez parler, veuillez lever la main sur Zoom. Lorsqu'on les invitera à parler, les participants virtuels pourront activer leur micro. Pensez à indiquer votre nom et la langue dans laquelle vous allez parler si ce n'est pas l'anglais. Parlez clairement et à un rythme raisonnable pour permettre une interprétation précise de vos propos. Je vais maintenant donner la parole au président du GAC, Nico Caballero. Merci.

NICO CABALLERO

Merci beaucoup, Julia. Bonjour à tous et bonjour à nos responsables thématiques, à nos invités. Nous avons Martin Kunc, membre- de l'équipe d'intervention en cas d'incidents liés à la

sécurité informatique. Nous avons Graeme Burton de l'Institut NetBeacon, Greg Aaron, du groupe de consultants Interisle. Nous avons également Susan Chalmers, bien sûr, qui appartient au groupe PSWG. Nous avons Janos Drienyovszki de la Commission européenne et nous avons Tomonori Miyamoto du Japon.

Bonjour à tous! Nous allons avoir des discussions intéressantes sur l'utilisation malveillante du DNS et je pense que nous aurons également la possibilité d'engager des discussions au niveau de tout le groupe. Je vais passer la parole d'abord à Tomonori.

TOMONORI MIYAMOTO Bonjour à tous. Bonjour, bonsoir à nos collègues présents ici et à ceux qui nous rejoignent en ligne. Je suis Tomonori Miyamoto, je suis représentant du Japon et je vais donc modérer les discussions d'aujourd'hui. Voilà l'ordre du jour. Après l'introduction, nous allons entendre des présentations sur le paysage de l'utilisation malveillante du DNS et de l'atténuation de cette utilisation malveillante. Nous aurons une présentation de Tchéquie sur une campagne d'hameçonnage et une autre présentation d'Interisle.

Ensuite, nous allons parler des prochaines étapes en matière d'élaboration de politiques et d'autres pistes de travail. Nous allons entendre une présentation sur la délégation des PDP. Ici, on a des informations de contexte par rapport aux discussions sur l'utilisation malveillante du DNS. Les RA et les RAA prévoient des dispositions en matière d'utilisation malveillante du DNS.

Il faut comprendre quel est le contexte de ce type de disposition. Donc la définition de l'utilisation malveillante du DNS dans les contrats est limitée aux logiciels malveillants, réseaux zombies, hameçonnage, dévoiement et spam lorsqu'il est utilisé pour véhiculer d'autres abus. Nous considérons donc qu'il s'agit d'un pas en avant pour essayer de lutter contre l'utilisation malveillante du DNS. Diapo suivante.

Certains d'entre vous connaissent déjà ce tableau ou cette diapo. Donc on voit que la portée du travail de l'ICANN en matière contractuelle correspond à la partie qui est en vert sur l'écran. Et donc, il faut considérer également cette relation avec les autres parties de l'écosystème. Nous devons donc envisager une coopération avec les parties prenantes qui se trouvent en dehors de ce schéma.

Vous voyez, donc la partie en vert correspond à des PDP potentiels qui pourraient être envisagés dans les années à venir. Diapo suivante, s'il vous plaît. Dans la réunion précédente à Seattle, nous avons passé en revue les preuves et les informations concernant l'atténuation de l'utilisation malveillante du DNS et nous avons eu un webinaire du GAC où nous avons une présentation de l'Institut Beacon sur l'utilisation malveillante du DNS et les idées possibles pour un PDP.

En plus, la petite équipe sur l'abus du DNS de la GNSO a également présenté ses objectifs et son calendrier. Aujourd'hui, dans les discussions, nous avons parlé de l'élaboration de politiques. Voilà

donc la dernière diapo de ma présentation. Ce n'est pas précis à 100 %, mais ça nous permet de voir un petit peu comment on s'organise au niveau des sujets à débattre en matière d'abus du DNS. Vous voyez que sur la droite, il y a donc plusieurs mesures qui peuvent être mises en œuvre de manière proactive.

Donc, en plus de ce qui est fait au niveau des contrats, comme je l'ai déjà dit, on pourrait mettre en place des mesures pour essayer de réduire le temps de réponse. Outre ces mesures, nous pouvons donc envisager des mesures proactives, y compris donc des activités de signalement, de surveillance et d'autres types d'activités dans ce sens.

Sur la base des résultats du rapport INFERMAL, nous pouvons donc voir quelles sont les informations obtenues en matière d'enregistrements groupés. Ensuite, je vais inviter Martin pour faire la présentation du pays hôte. Martin, vous avez la parole.

MARTIN KUNC Je suis là pour vous présenter un cas d'hameçonnage que nous avons eu dans notre pays. Je vous parle un petit peu de nos projets les plus importants sur le Routing Demon Bird et les mesures du DNS que nous appelons ADAM. Diapo suivante.

Qui sommes-nous? Nous sommes l'opérateur de registre du domaine .CZ. Donc moi en tant qu'analyste de sécurité, je représente ce groupe ici. Donc nous avons commencé notre travail en juin 2022. Donc, nous avons eu un cas d'hameçonnage pour le

.CZ. C'est quelque chose de pas habituel. Et donc cet hameçonnage a voulu et fait en sorte que nous puissions leur donner de l'argent en échange de ces activités malveillantes. Donc nous avons ici le logo de notre ministère.

Ensuite, il y a quelque chose qu'on appelle BankID. Je sais que ce n'est pas fréquent dans d'autres pays, mais les banques se sont réunies et ont mis en place quelque chose qui s'appelle BankID pour utiliser les mêmes identifiants et mots de passe pour accéder dans les sites gouvernementaux et les banques. Et donc nous avons après les acteurs malveillants.

Alors, quel est le scénario de cette activité d'hameçonnage? C'est assez ordinaire. Les gens reçoivent un SMS qui leur dit : Vous pouvez obtenir de l'argent. Ici, ils cliquent sur le lien. Et à ce moment-là, on leur demande de l'argent. Il y a un certain nombre de ce type de SMS. Comme vous le voyez ici, je sais que vous ne pouvez pas lire ce qui est écrit là, mais le message est à peu près le même, à savoir Cliquez ici, vous avez recevoir de l'argent. Une fois que vous avez cliqué sur le lien, vous devez saisir vos identifiants bancaires ou d'autres types d'autorisation et d'authentification, mais ils vous demandent surtout les identifiants et mots de passe bancaires.

Cela est uniquement possible pendant les heures normales de travail. Et donc vous pouvez accéder uniquement à ces sites pendant ces horaires-là. Il avait donc besoin de ce type d'activité

parce que l'acteur malveillant utilisait donc ces identifiants en temps réel pour obtenir une confirmation.

Voilà un exemple de site qui a l'air légitime. Bien sûr, mis à part l'URL. Et si vous voyez un autre exemple ici, vous pouvez choisir la banque. Vous ne pouviez pas choisir n'importe quelle banque. Il y avait un choix à faire. Et si vous le voyez sur l'URL à gauche en haut, vous voyez donc le type de campagne qui était mené.

Ici, vous voyez donc un autre site en 2022. Nous avons recensé 11 cas et deux domaines par mois, ce qui était assez peu fréquent. En février 2023, nous avons recensé 72 domaines en un seul mois, ce qui faisait beaucoup. Mais à ce moment-là, nous étions prêts. Nous pouvions mettre en place des mesures. Nous savions qu'ils s'amélioreraient en permanence et nous, nous avons essayé de nous améliorer à notre tour. Nous avons commencé donc à mettre en place une recherche active. Nous avons essayé d'améliorer nos processus et nous avons beaucoup étudié.

Parmi les exemples de recherche active, nous avons pu rechercher des zones et nous avons vu quels domaines étaient enregistrés. Nous avons utilisé des caractères similaires à ceux qu'ils utilisaient parce qu'ils avaient besoin de changer et d'avoir de nouvelles idées, de nouveaux noms. Donc à la fin, nous avons pu identifier par exemple des domaines enregistrés sous le nom Last Week.

Cela nous a aidés à avoir et à dresser une liste de domaines qui pourraient faire l'objet d'activités d'hameçonnage. Nous avons mené des tests et nous avons vu que notre adresse IP n'était jamais

bloquée et nous avons donc vu que lorsqu'un site malveillant était en fonctionnement, nous pouvions recevoir des notifications pour savoir quand est-ce qu'il était actif.

Nous avons donc pu recevoir ce type de notifications et nous avons pu réduire le délai de suspension de ces domaines, ce qui était un point crucial pour nous. Nous avons pris des notes, bien sûr, par rapport à ce que nous avons découvert. Et donc les sites web étaient créés quelques jours après l'enregistrement, parce que tout d'abord, il fallait enregistrer le domaine, obtenir les enregistrements DNS, et une fois que tout était prêt, il permettait une liste d'annuaires de leur côté.

Et, très souvent, nous avons pu extraire ce fichier du DNS et l'analyser. Les exemples étaient parfois similaires, parfois ils étaient différents parce qu'ils s'amélioraient et donc très très vite, ils pouvaient activer leur site web.

Si vous êtes curieux, nous avons pu retrouver le sous domaine et nous avons pu donc voir quelles étaient toutes les sessions qui étaient créées. Mais, nous avons pu également utiliser la transparence des certificats pour trouver des domaines qui n'étaient pas visibles pour nous avant. Diapo suivante. Et finalement, nous avons réussi à avoir une victoire parce que nous avons pu arrêter ces activités pour n'en venir qu'à 28 domaines compromis en mars 2023.

Et, depuis, nous voyons que ces chiffres restent assez stables. Bien sûr, il y a des tentatives, mais il n'y a pas eu d'activité aussi

importante que celle qu'on avait pu constater auparavant. C'est un schéma un peu difficile à comprendre, mais je vais essayer de vous expliquer. La partie en vert correspond à la période où les sites ont été résolus de manière correcte. Ces sites, excusez-moi, n'ont pas été résolus correctement. C'étaient des sites malveillants.

Et, ensuite, vous voyez, pour le reste, c'est des sites qui ont été résolus. Il est important de dire que ce n'est pas le nombre d'utilisateurs réels, parce que nous ne voyons pas combien d'utilisateurs se trouvent derrière un résolveur, mais cela nous donne au moins une estimation. Par rapport aux chiffres dans ce sens. Ici, vous voyez donc en vert que nous nous sommes améliorés et c'est pourquoi nous considérons que c'est une espèce de victoire de notre part.

Alors, en coulisses, qu'est-ce qui se passait? Nous avons l'article 17 dans notre législation qui nous permet d'enlever les domaines de la zone s'ils bouleversent la sécurité. Nous pouvons donc les extraire de la zone pendant un mois, et cela nous donne suffisamment de temps pour donner au propriétaire du domaine la possibilité de voir ce qui se passe et de venir nous voir pour expliquer ce qui peut se passer dans son site par exemple.

Et, s'il y a une activité malveillante, nous pouvons les conseiller par rapport à la manière d'en venir à bout. Il y a également une liste publique de domaines qui sont bloqués. C'est tout de mon côté, donc j'espère que vous avez trouvé cette présentation intéressante et je suis prêt à répondre à vos questions.

TOMONORI MIYAMOTO Merci beaucoup pour cette présentation Martin. Maintenant, nous allons ouvrir le micro à des questions. Est-ce qu'il y a des questions?

GABRIEL ANDREWS Bonjour, je suis Gabriel Andrews. Merci beaucoup pour cette présentation Martin. J'étais vraiment intéressée. Ça a été intéressant et j'ai été impressionnée quand vous avez parlé de la reconnaissance de domaine qui était enregistré à des fins malveillantes et vous avez parlé également de la manière dont ces sites se mettaient en ligne, de la manière dont vous étiez alertés.

Si j'ai bien compris, c'était une mesure très proactive. Je me demande est-ce que vous avez senti qu'il fallait attendre à recueillir suffisamment de preuves avant de pouvoir agir?

MARTIN KUNC Oui, à l'époque, nous avons attendu d'avoir suffisamment de preuves pour éviter qu'il s'agisse d'un projet de recherche par exemple. Et, donc, notre processus est mis en place de telle sorte que si nous voyons qu'il y a des preuves suffisantes. Nous sommes en mesure de bloquer le site.

GABRIEL ANDREWS Je ne pense pas avoir entendu parler d'une mesure aussi proactive. Je suis extrêmement impressionné. C'est très intéressant de voir

tout cela. Je sais qu'il y a eu des difficultés par le passé parce que parfois on sait qu'il y a des domaines qui seront utilisés à des fins d'hameçonnage, mais on n'a pas suffisamment de preuves et c'est une difficulté.

Donc, le fait de pouvoir faire ce type de surveillance et établir certaines règles pour agir de manière proactive, je trouve que c'est vraiment intéressant. Merci beaucoup.

MARTIN KUNC Merci beaucoup. Et, juste pour vous dire que nous avons fait beaucoup de campagnes d'hameçonnage qui nous ont permis de comprendre l'importance de ce travail, de pouvoir détecter les domaines qui seront utilisés à des fins d'hameçonnage. Parce que sinon nous ne pouvons pas faire les rapports. Donc, il est très important de faire cela.

TOMONORI MIYAMOTO Nous avons Ashwin.

ASHWIN SASONGKO SASTROSUBROTO Oui. Bonjour, Ashwin d'Indonésie au micro. Merci beaucoup pour la présentation. J'avais quelques questions. Quelle est l'efficacité de l'utilisation du DNSSEC et du secure DNS dans votre site web? Et, est-ce que les utilisations des documents de l'ICANN sont utiles dans vos travaux?

Et ensuite, pour Martin. Vous avez parlé de questions d'hameçonnage et vous utilisez le ccTLD .cz ou est-ce que vous utilisez le gTLD .org?

MARTIN KUNC

Est-ce que vous pourriez répéter la première question? Parce que je ne suis pas sûr de l'avoir comprise. Mais alors, pour vous répondre à la deuxième, nous nous sommes bien sûr concentrés davantage sur le domaine .cz. C'était plus simple pour nous de faire ce suivi de ce nom de domaine. Mais bien sûr, nous avons des cas d'hameçonnage qui utilisent n'importe quel type de domaine, mais ils ne sont jamais aussi gros que ce point-là.

ASHWIN SASONGKO SASTROSUBROTO

Alors, ma première question portait sur le fait qu'un site web de l'ICANN doit utiliser le DNSSEC. Et, quelle est son efficacité? Est-ce que l'utilisation l'application du DNSSEC permet d'atténuer les risques liés à l'utilisation malveillante du DNS? Parce que, par exemple en Indonésie ou dans d'autres pays, je me rappelle, on a parlé dans les SO et les AC. Nous avons produit les normes de 2021 du système de sécurité. Est-ce que vous attendez que cette certification 27001 soit utile contre l'utilisation de la valeur du DNS?

MARTIN KUNC

Alors, le DNSSEC ne sert pas à au travail de lutte contre l'hameçonnage. Je ne connais pas vraiment les normes ISO, donc

je ne pense pas être la personne la mieux placée pour répondre à cette question. J'en suis désolé.

TOMONORI MIYAMOTO Aderonke, vous avez la parole.

ADERONKE ADENIYI Alors, j'ai une question pour Martin, donc votre présentation était formidable. C'est tout à fait nouveau pour moi. Donc, j'ai une question. Pardon. Je m'appelle Aderonke et je viens du Nigéria. Ma question portait sur les BankID.

Est-ce que vous pensez que le régulateur des banques peut jouer sur l'atténuation des abus du DNS? Puisqu'il y a des identifiants qui sont partagés par toutes les banques sur toutes les plateformes numériques. Mais, je voulais savoir si vous avez travaillé main dans la main avec les régulateurs des banques pour faire face à ces questions d'identifiants?

MARTIN KUNC Alors, de mon point de vue, nous n'avons pas vraiment réussi à rentrer en contact avec les banques. Mais heureusement, ils se sont mis à travailler également de leur côté pour permettre de contacter les utilisateurs de ces tentatives d'hameçonnage. Donc, ils leur ont envoyé des notifications pour leur dire qu'il y avait un danger probable, donc ils ont fait de leur mieux.

TOMONORI MIYAMOTO Merci beaucoup. Nous allons donc passer à notre prochaine partie. Je vais demander à Karen et Greg de Interisle de nous faire leur présentation.

KAREN ROSE Merci beaucoup [Inaudible]. Bonjour à tout le monde, Je suis Karen Rose et voici Greg Aaron. Nous travaillons au groupe de consultants Interisle. Nous avons plus d'une vingtaine d'années d'expérience et nous sommes très heureux d'être ici avec vous aujourd'hui. Ces dernières cinq années, nous avons fait des recherches sur l'utilisation malveillante du DNS et le crime en ligne.

Et, aujourd'hui, on nous a demandé de nous concentrer sur l'utilisation malveillante du DNS et l'hameçonnage, mais vous pouvez trouver un rapport bien plus large sur tous ces enjeux sur notre site internet. Donc, prochaine diapositive s'il vous plaît. Ce qui est important à retenir, c'est que malheureusement, l'hameçonnage et l'utilisation malveillante du DNS augmentent de manière très inquiétante. Nous enregistrons plus de 2 millions d'attaques d'hameçonnage… ont été identifiées ces dernières années. Donc, cela, c'est une augmentation de 425 % de ces sur ces cinq dernières années.

Et, c'est encore une fois une sous-estimation, parce qu'il y a tellement de tentatives d'hameçonnage et d'attaques qui ne sont pas enregistrées. 77 % de ces de ces domaines d'hameçonnage ont été enregistrés à des fins malveillantes et l'hameçonnage a un coût très important pour la société. Plus de 18 000 $ sont enregistrés par

minute d'hameçonnage. Et bien sûr, encore une fois, c'est une sous-estimation puisque beaucoup de tentatives d'hameçonnage ne sont pas enregistrées. Ce qui est important à retenir, c'est que les efforts d'atténuation de l'utilisation malveillante du DNS sont pour le moment inefficaces.

Et, si vous vous demandez quelle est cette baisse que vous voyez à l'écran? C'était lors de la clôture d'un site d'une entreprise qui s'appelait Freenum. Et bien sûr, cette clôture de ce site a fonctionné pendant un temps, mais vous voyez que les tentatives d'hameçonnage ont augmenté très rapidement à la suite de cela. Les hameçonneurs ont tendance à exploiter deux choses dans les noms de domaine les coûts très bas et l'enregistrement facile.

Ce que les hameçonneurs préfèrent, ce sont les sites qui coûtent 2 $ au maximum. Et, ces coups bas sont assez courants dans les nouveaux gTLD. Et, cela augmente une possibilité d'hameçonnage. Si vous voyez ici à l'écran, vous voyez la part de marché total des nouveaux gTLD en jaune. Cela ne représente que 11 %. Pourtant, si vous regardez le camembert d'en dessous, vous voyez que les nouveaux gTLD représentent 51 % de tentatives d'hameçonnage cette année.

Donc, bien sûr, le .com et .net sont très attractifs pour les hameçonner évidemment, puisqu'ils représentent 32 % des tentatives d'hameçonnage. Ce que les utilisateurs malveillants peuvent faire, c'est utiliser des promotions, des offres groupées de la part des bureaux d'enregistrement. Les hameçonneurs

exploitent également des bureaux d'enregistrement et des TLD qui ne demandent que très peu de validation ou de vérification d'identité à l'enregistrement.

Les hameçonneurs préfèrent certains fournisseurs également, par exemple comme des bureaux d'enregistrement ou des TLD qui sont au carrefour entre la facilité et les coûts très bas. Donc, je ne peux pas faire le classement de ces dix dernières années, mais nous voyons vraiment une augmentation des tentatives d'hameçonnage pour les entreprises qui sont dans les tops cinq et dix.

Les noms utilisés par les hameçonneurs sont très difficiles à repérer. Je vous ai montré ici quelques exemples. À gauche, vous voyez des tactiques qui sont donc de générées automatiquement et algorithmiquement des noms avec des chaînes de caractères qui sont complètement aléatoires, donc des noms…

Ou sinon, une autre solution est d'utiliser des noms qui ressemblent à des marques connues par les utilisateurs et d'utiliser également des informations erronées. D'autres outils peuvent être de répéter ces modèles et certains ccTLD ont des systèmes en place pour évaluer en amont les adresses et de garantir une vérification.

GREG AARON Donc, tous les ans, nous travaillons sur l'évaluation et l'enregistrement des situations d'hameçonnage et en général les hameçonneurs n'enregistre pas un ou deux domaines en même temps. Ils utilisent un ensemble de domaines. Donc, si vous

regardez certains noms de domaine qui sont enregistrés au même moment par le même bureau d'enregistrement.

On estime que 37 % de ces noms de domaines utilisés pour l'hameçonnage sont des noms de domaine utilisés en masse. Nous pouvons évaluer ceux qui sont utilisés pour l'hameçonnage, mais en réalité, il y a d'autres noms de domaine dans ces sets qui ont des objectifs que nous ne connaissons pas. Il est toujours très difficile de comprendre et de tirer les données. Parfois, certains de ces ensembles sont très larges. L'année dernière, nous avons vu un ensemble de 17 000 noms de domaine qui étaient utilisés par un seul hameçonneurs.

L'idée, c'est que les hameçonneurs travaillent de plus en plus vite. Les victimes sont victimes d'une tentative d'hameçonnage dans les 8 h après le lancement d'un site. Donc, les hameçonneurs savent qu'ils vont se faire attraper, mais l'objectif est d'aller le plus vite possible. Nous voyons de plus en plus de noms de domaine utilisés et cela est possible grâce à l'automatisation.

Les utilisateurs malveillants peuvent donc perpétrer des attaques continuellement et cela leur garantit des profits. Et, tant que le site est en ligne, les profits continuent d'arriver pour eux. Et, s'il y a tellement de tentatives d'hameçonnage, c'est parce qu'en réalité elles sont toujours couronnées de succès. Donc, il faut se poser la question de pourquoi cela existe, pourquoi nous avons cette situation.

KAREN ROSE

L'utilisation malveillante du DNS est possible à cause de choix. Ce sont les choix que l'ICANN prend dans ses politiques et les normes de détermination de fonctionnement du marché. Les choix des entreprises qui décident de mener à bien leurs affaires. Nous nous sommes rendu compte que la concurrence est une bonne chose. Donc, nous avons l'habitude de dire que la concurrence est une bonne chose, mais d'un point de vue économique, ce n'est pas toujours le cas.

Le fait qu'il n'y ait pas de règlement raisonnable, la sur concurrence peut avoir des conséquences négatives. Et en réalité, l'utilisation malveillante du DNS, c'est l'équivalent de la pollution industrielle pour l'industrie. Cela crée des dommages dans la société et pour les utilisateurs finaux. Le marché du DNS est très compétitif. Aujourd'hui, il y a plus de 2000 bureaux d'enregistrement, plus d'une centaine de TLD ouverts. Et pour les criminels, les noms de domaine, ce sont des biens communs. Ils sont très facilement interchangeables et ils peuvent être utilisés par l'industrie a un coût quasiment nul.

Donc, pour mettre en place des politiques anti utilisations malveillantes, cela demandera une analyse des dynamiques de marché et de faire des choix. Ce dont nous avons besoin, ce sont des mesures proactives qui permettent d'empêcher l'utilisation de la valeur du DNS avant même qu'elle ait lieu, pas seulement d'atténuer les dommages, mais d'atténuer l'utilisation

malveillante du DNS des domaines, même si l'atténuation a posteriori sera toujours utile.

Et, il est toujours important de voir comment les politiques sont prises. Parce que lorsqu'un nouveau gTLD rentre dans le marché, cela va… Plus il y a de noms de domaines qui rentrent sur le marché, plus cela va amener les prix à réduire et plus il y aura de concurrence. Et, si rien ne change, les données que nous vous avons montrées au début de la présentation continueront d'augmenter.

GREG AARON L'une des tendances que nous voyons en particulier en Europe, c'est que les opérateurs de registre font de nouvelles choses désormais. Certains, par exemple, ne demandent pas toujours aux titulaires de noms de domaines de prouver leur identité à l'achat, mais cela entraîne des risques. Par exemple, nous avons vu beaucoup d'opérateurs de registre qui nous disent que les enregistrements en masse sont un exemple de risque.

Et, les titulaires de noms de domaine arrivent. Nous ne savons pas qui ils sont, mais ils enregistrent énormément de noms de domaine. Donc, peut-être que nous devrions leur demander de justifier leurs identités et cela pourrait être une solution. Mais, ceci est une approche basée sur les risques qui a désormais lieu dans certains TLD européens. Bien sûr, les prérequis sont assez… Les

prérequis de l'ICANN pour le moment sur la vérification sont assez minimes.

Nous avons trouvé que 21 % des bureaux d'enregistrement ne demandez pas d'étape de vérification d'identité à l'enregistrement. Donc, nous pensons que ceci est une opportunité de d'évaluer une approche basée sur les risques, donc de faire des vérifications a priori, de faire de la prévention pour empêcher les criminels d'agir.

Alors, notre idée ici de pouvoir avoir une discussion, c'est d'améliorer les prérequis de vérification, d'évaluer les problèmes liés à l'enregistrement en masse. Ce sont deux types de problèmes qui vont main dans la main en réalité. Un autre point qui est important à prendre en compte, c'est que les contrats de l'ICANN demandent aux opérateurs de registre de travailler avec tous les bureaux d'enregistrement accrédités auprès de l'ICANN. Et, l'objectif était de s'assurer que les entreprises n'essaieraient pas de s'avaler les unes les autres. Et, nous voulons bien sûr un environnement compétitif, mais les opérateurs de registre doivent travailler avec des bureaux d'enregistrement qui parfois amène des situations dangereuses.

Et, ça, c'est une situation qu'il nous faut évaluer parce que dans ce cas-là, l'opérateur de registre se retrouve dans une situation inconfortable et il y a beaucoup de titulaires de noms de domaine qui arrivent alors qu'ils auraient voulu peut-être éviter cette situation.

Bien sûr, les opérateurs de registre et les bureaux d'enregistrement ont beaucoup d'outils qu'ils peuvent utiliser. Il y a beaucoup d'expériences qui sont mises en place pour trouver les domaines malveillants avant qu'ils rentrent en activité. Donc, il y a des discussions, il y a des outils et des solutions qui existent et il y a également des politiques qui pourraient améliorer la situation.

KAREN ROSE

Nous avons de nouveaux rapports remplis de données qui seront publiés au troisième trimestre de cette année. Si vous souhaitez vous référer à nos rapports, je vous rappelle que notre objectif n'est pas seulement d'évaluer les noms de domaine, mais également l'utilisation malveillante sur les hôtes, sur les sous hôtes et l'hameçonnage, et les logiciels malveillants. Donc, nous avons nos rapports disponibles sur nos sites web.

Nos sources, nos méthodologies et nos données supplémentaires sont sur un site internet qui est le site internet du cybercrime du réseau Cybercrime qui est un site internet qui nous permet de rassembler toutes nos informations. Nous sommes également disponibles sur Substack. Nous publions un post tous les deux trois jours, Donc vous pouvez vous y référer. Notre site internet est évidemment affiché ici et notre adresse mail est également disponible si vous souhaitez rentrer en contact avec nous. Merci beaucoup.

TOMONORI MIYAMOTO Merci beaucoup pour cette présentation. Puisque nous n'avons pas beaucoup de temps, nous allons passer à la présentation suivante et si vous avez des questions, n'hésitez pas à contacter les intervenants. Maintenant, je vais passer la parole à Janos.

JANOS DRIENYOVSZKI Nous allons passer donc à la question des PDP et des micro PDP potentiels que l'on pourrait élaborer. Je vais donner la parole à Graeme de NetBeacon.

GRAEME BUNTON Je m'appelle Graeme Bunton, je suis PDG de l'Institut NetBeacon. Ça fait partie de l'opérateur de registre qui exploite le .org à but non lucratif. Nous avons publié un papier blanc qui propose cinq idées de PDP potentiels. Je voulais donc vous présenter cela.

Je n'ai pas énormément de temps. Je ne vais pas rentrer dans le détail de ces idées en matière de PDP, mais je vais vous donner un aperçu et je vais vous donner le lien vers le document qui fait une vingtaine de pages pour que vous puissiez voir les détails. Alors, diapo suivante Pourquoi nous avons mené ce travail? l'Institut NetBeacon passe toute la journée, tous les jours pour voir comment réduire l'utilisation malveillante du DNS. Nous faisons partie également de la Chambre de parties contractantes. Nous avons certaines obligations, nous travaillons donc un petit peu comme le fait Interisle.

Nous avons un projet pour mesurer et comprendre l'abus du DNS dans l'écosystème. Ça s'appelle la carte NetBeacon. Nous avons également un service centralisé où nous voyons des dizaines de milliers de signalements d'abus. Et donc, en nous basant sur toutes ces données, je dois parler le plus lentement. Je m'excuse.

Nous voulons voir donc, à partir de ces données, comment nous pouvons aider à renforcer ce dialogue par rapport à cette question. Nous pensons que nous devons pouvoir arriver à un résultat de manière opportune et montrer à cette communauté ce que nous considérons comme quelque chose de faisable des PDP, des petits PDP ou des PDP plus réduits. Donc, vérification des domaines associés. Ce devrait être une obligation liée à tout signalement d'abus.

Par exemple, recevoir des preuves par rapport à l'utilisation malveillante d'un domaine et à ce moment-là, il faudrait vérifier qu'il n'y ait pas d'autres domaines associés à cette utilisation malveillante. Donc, une vérification à faire. Ensuite, les API qui servent de lien. Donc, à partir du rapport INFERMAL. Et merci d'ailleurs à l'OCTO de l'ICANN pour ce rapport.

C'est qu'il y a des API qui n'ont pas de passerelle. Et donc… Donc, ce type d'enregistrement et 401 % plus probable qu'elles fassent l'objet d'abus. Et, donc, il y a certains outils qui permettent ce type de comportement, d'enregistrement groupé. Diapo suivante. Donc, des contacts en matière d'abus de sous-domaines. Donc, voir si les obligations qui existent au niveau des opérateurs de

registre peuvent être appliquées aux opérateurs de registre qui offrent des sous-domaines à des parties tierces.

Ensuite, quatre mécanismes de recours des titulaires de noms. Lorsque les différentes parties travaillent de manière conjointe, elles peuvent arriver à des résultats à échelle. Et, donc, il faudrait faire en sorte que l'on puisse résoudre les erreurs qui pourraient être faites ensuite. Coordination réseau zombies et DGA. En ce moment, les réseaux zombies travaillent à l'élaboration d'algorithmes pour la génération de noms de domaine et les forces de l'ordre travaillent de manière indépendante et cela n'est pas efficace.

Ce que nous proposons, c'est une fonction centralisée au sein de l'ICANN pour collecter et disséminer ce travail pour arriver à mieux gérer les réseaux zombies. Alors, les conclusions, je pourrais en parler de manière individuelle. Je pourrais parler de ces PDP de manière individuelle. Je pourrais le faire si vous voulez me contacter dans les couloirs.

Mais, je pense qu'il y a un certain nombre de conclusions qui sont clés et que je voudrais vous présenter. Il y a une opportunité ici maintenant de pouvoir avancer au sein de cette communauté sur des PDP, c'est à dire des élaborations de politiques pour faire une différence au niveau des abus du DNS, mais nous devons nous assurer que nous travaillons de manière collective pour pouvoir mener à bien des processus qui aient une portée limitée et limitée

dans le temps également. Pour progresser, il faudra bien cibler nos efforts et cette cible doit être vraiment très précise.

Nous savons que ça peut être complexe, mais il y aura des impacts opérationnels. Mais, nous pouvons obtenir de bons résultats. Nous pouvons obtenir des résultats progressifs et c'est mieux que rien. Je pense que la taille de la bouchée que nous prenons est en lien direct avec la capacité que nous avons à mastiquer. Donc, je pense que le fait de pouvoir prendre des petites bouchées nous permettra donc d'aller petit à petit plus loin.

Et finalement, dernière conclusion. Et, cela rejoint ce que vient d'être dit par Interisle, c'est que nous devons passer des signalements individuels d'abus à une gestion des abus du DNS à échelle. Les rapports qui ont été faits l'année dernière sont excellents. Nous, dans nos données, on voit tout le temps ces activités malveillantes qui ne font que s'accroître. Mais, on ne peut pas rester au niveau individuel de signalement d'abus.

Donc, deux propositions d'un côté, la vérification des domaines associés et la vérification des enregistrements groupés. On peut voir comment nous pouvons avancer de manière responsable et facilement pour ne pas rester à la gestion individuelle des signalements d'abus, mais passer à des campagnes plus larges de gestion ou de lutte contre l'utilisation malveillante. Je pense que c'est à cela que la communauté doit réfléchir. Nous avons publié ce document dont je vous ai parlé avant.

La communauté, à des idées, à des idées plus ciblées, des idées qui pourraient être couronnées de succès, mais il faut que l'on identifie de manière très ciblée la portée de notre travail. Nous savons qu'il y a beaucoup de discussions et nous devons donc avancer sur ces idées. Merci beaucoup de m'avoir donné l'opportunité de parler et je vous repasse la parole.

NICOLAS CABALLERO Je vais redonner la parole à Tomori et je vais demander à nos représentants du GAC de prendre en considération ce besoin d'agir de manière rapide parce que ces acteurs malveillants nous regardent en ce moment même. Et, si dans cinq ans on finit notre PDP, ils seront déjà prêts. Ils sont toujours… Ils ont une longueur d'avance par rapport à nous. Donc, je pense que nous devrions agir rapidement. Tomori, vous avez la parole. Pardon! Janos.

JANOS DRIENYOVSZKI Maintenant, passons à ce que nous pensons que Le GAC pourrait faire en matière de PDP ciblé. Je voulais passer en revue très brièvement des idées présentées par la chambre des parties contractantes hier dans une réunion. Il y a quatre idées. Je pense que c'est une discussion très efficace pour nous aujourd'hui.

L'une des idées, c'était d'avoir des signalements exploitables d'utilisation malveillante du DNS pour pouvoir identifier d'autres activités malveillantes sur le même compte. Ensuite, des mesures proactives pour faire en sorte que ces opérateurs de registre qui

offrent des API mettent des mesures supplémentaires en œuvre, des mesures supplémentaires.

Ensuite, avoir un cadre opérationnel pour identifier des botnet ou des réseaux zombies qui génèrent des algorithmes et finalement une amélioration de la qualité des signalements. Alors des idées pour réfléchir à d'autres pistes de travail. Parmi ces idées, il y a donc des mesures proactives.

Nous en sommes à un moment où nous essayons d'explorer des mesures réactives et préventives. Comme Nico l'a dit, l'objectif est d'aboutir à des résultats plus rapides avant le lancement de la nouvelle, la prochaine série de nouveaux gTLD. Nous devrions établir une priorité parmi les actions spécifiques que nous pouvons mettre en place. Et ensuite je vais parler des PDP ciblés.

Dans le communiqué de Seattle, le GAC a considéré qu'il était important de se pencher sur la question des enregistrements groupés de noms de domaine, car ce type d'enregistrement est directement lié aux signalements d'utilisation malveillante du DNS. Donc ces enregistrements groupés représentent un risque important d'être associés avec des comportements malveillants.

Et, le rapport INFERMAL a également mis en lumière ce type de liens et c'est pour cela que nous devrions nous focaliser sur ce type d'enregistrement groupé. Une idée pourrait consister à demander aux parties contractantes de mettre en œuvre des mesures proactives concernant les enregistrements groupés.

Cela peut inclure, restreindre l'enregistrement par le biais d'un API Et restreindre l'enregistrement par certains utilisateurs. Et pour cela, une vérification au niveau des titulaires de noms pourrait être mise en œuvre. Nous pourrions également augmenter les prix des enregistrements groupés en fonction du volume, etc.

Donc, ces mesures proactives pourraient compléter les mesures réactives qui sont déjà en place et qui figurent dans ces contrats que propose la Chambre des parties contractantes. NETBeacon propose également de vérifier les domaines associés. De cette manière, nous pourrions combiner ces mesures réactives et préventives.

Maintenant lorsqu'on passe à d'autres mesures proactives. Dans le communiqué de Hambourg, le GAC a réitéré l'importance de surveiller des mesures proactives et de mettre en place des pratiques pour s'attaquer au problème de l'abus de DNS. Et le GAC a encouragé l'utilisation de systèmes de détection d'abus.

En ce sens, la surveillance des comportements malveillants est un autre domaine à explorer. Cela veut dire identifier des actions qui sont liées à des activités malveillantes. Cela figure dans la recommandation 1 de la petite équipe sur l'abus de DNS en octobre 2022. Cela veut dire que tous les enregistrements qui présentent un certain niveau de risque devraient faire l'objet d'une vérification d'identité.

Ici, on a des exemples de l'espace ccTLD en Europe avec l'utilisation de systèmes de détection power DNS. Une autre

mesure pourrait être la vérification d'identité dans le cycle de vie de domaine, c'est-à-dire revérifier lorsque le domaine est renouvelé par exemple. Maintenant, je vais passer la parole à Susan.

SUSAN CHALMERS Merci beaucoup, Janos. Je vais très brièvement vous parler de la troisième idée qui a été présentée par rapport à l'idée de mettre en place un PDP. Et cela concerne les obligations de signalement. Des politiques robustes sont basées sur des preuves qui permettent de considérer des politiques à l'ICANN. Cela concerne des informations collectées par le biais de certaines plateformes de l'ICANN. L'Institut NetBeacon nous fournit des informations également.

On peut également lire des rapports de certains organismes comme Interisle, le rapport INFERMAL également, dont on a bien discuté lors de notre réunion à Seattle. L'ICANN produit également des rapports concernant l'abus du DNS et nous avons donc une idée assez précise de la manière dont les parties contractantes mettent en œuvre les obligations de 2024 en matière d'abus de DNS qui figurent dans leurs contrats.

Or, il n'y a pas d'obligation pour les parties contractantes de publier leurs activités en matière d'atténuation de l'utilisation malveillante de DNS. Donc une idée peut être de mettre en place des rapports statistiques pour les parties contractantes. Une autre

suggestion. C'est une autre suggestion que l'on pourrait ajouter aux idées qui ont été identifiées hier. Diapo suivante, s'il vous plaît.

Vous voyez ici les prochaines étapes des pistes à explorer par l'ICANN. Si vous avez participé au webinaire qui a eu lieu en amont de l'ICANN 83, nous avons eu une présentation de la petite équipe de la GNSO sur l'abus du DNS. Cette équipe commence à travailler pour évaluer les efforts d'atténuation de l'abus du DNS, pour déterminer s'il y a besoin de mettre en place des PDP. Les recommandations seront finalisées en septembre et un rapport final devrait être publié en octobre.

Nous savons que ce calendrier pourrait être raccourci et nous avons hâte de voir le résultat de ce travail. Nous allons avoir la petite équipe aujourd'hui et nous allons donc savoir quel est le progrès du travail de cette équipe. Nous aurons une réunion bilatérale avec le conseil d'administration aujourd'hui et je demanderais donc au personnel de l'ICANN de montrer la diapo qui montre la question que nous allons poser au conseil d'administration. Donc, je pense que, en général, les collègues de l'ICANN seront d'accord sur le fait que les PDP devront durer moins longtemps. Certains PDP durent des années.

Donc la question que nous allons adresser au conseil d'administration, et cela ne concerne pas spécifiquement l'abus du DNS, mais nous voudrions savoir comment pourrions-nous apporter un changement au niveau des PDP afin que les résultats puissent être vus plus vite? Parce que cinq ans, 10 ans, ça fait

beaucoup. Pourquoi pas 12 mois? Alors, voilà une idée sur laquelle j'attire l'attention des représentants du GAC cet après-midi.

Maintenant, beaucoup des représentants du GAC connaissent déjà la manière dont les représentants du GAC peuvent participer à l'élaboration de la politique de l'ICANN. Pour certains qui viennent de nous rejoindre, je vais très brièvement passer en revue ce processus. Tout d'abord, on va parler du processus d'élaboration de politiques. Le processus d'élaboration de politique multipartite de l'ICANN comprend la participation de toutes les parties de la communauté, y compris les représentants de l'ICANN.

Les PDP donnent lieu à des politiques de consensus. Ces politiques de consensus font partie des contrats et des dispositions contraignantes de ces contrats. Pour changer des politiques à l'ICANN, les politiques l'ICANN peuvent donner lieu à des amendements des contrats entre l'ICANN et les bureaux d'enregistrement et les opérateurs de registre. Mais ce processus d'élaboration de politique multipartite prévoit que tout amendement soit négocié de manière bilatérale avec les parties concernées.

C'est ce qui a été fait avec les amendements de 2024 qui sont entrés en vigueur en avril, le 1er avril de l'année dernière. Et donc ces dispositions établissent des obligations pour les opérateurs de registre et les bureaux d'enregistrement, mais sont le fruit de longues discussions entre les parties concernées. Il y a eu un commentaire public par rapport aux amendements proposés, mais

contrairement au PDP, ce n'est pas comme les PDP où ni l'ICANN, ni les parties contractantes sont concernées par le processus.

Bien sûr que l'avis du GAC est très important au niveau du PDP. L'avis du GAC, lorsqu'il est adressé au conseil d'administration, est un outil très important pour déclencher des changements au niveau des politiques de l'ICANN. Voilà un petit aperçu, notamment pour les nouveaux représentants du GAC. Diapo suivante, s'il vous plaît. Je pense qu'il nous reste une quinzaine de minutes, c'est ça? Nous voulons réserver un peu de temps pour la discussion du GAC.

Le président, comme à son habitude, a lancé un appel à thématique avant l'ICANN 83 et la question de l'abus du DNS figure parmi ces sujets d'intérêt. Nous avons fourni un texte par rapport pour cette question. Donc voilà, vous voyez sur l'écran les titres de ce texte que nous avons proposé. Pour la section Questions d'importance, nous allons parler et nous avons parlé de questions qui figurent sur l'écran.

Donc, révision du paysage de l'atténuation et de l'abus du DNS et les nouveaux PDP. Nous suggérons d'encourager des PDP ciblés au niveau de la portée, au niveau du temps pour avoir des résultats plus rapides. Nous voulons donc faire passer cette idée auprès des représentants du GAC. Nous voulons sensibiliser les collègues à cette question et pour cela, nous ouvrons le micro pour le débat.

NICO CABALLERO

Merci beaucoup, États-Unis. Pouvons-nous revenir en arrière à la diapo 12, s'il vous plaît? Oui. En ce qui concerne. Avant de passer la parole à l'Indonésie, l'Indonésie, excusez-moi. C'est une ancienne main ou voulez prendre la parole, Ashwin? C'est une ancienne main? Donc, avant de donner la parole à l'Indonésie et avant d'ouvrir le micro pour des questions et des commentaires, je voulais attirer votre attention sur un aspect. Le PDP – le processus d'élaboration de politiques – permet aux membres du GAC une participation. Lorsque vous vous sentirez à l'aise, vous avez l'opportunité de participer de manière significative à ce processus d'élaboration de politiques.

Donc l'idée, c'est… Je veux dire, pourquoi pourrait-on participer à ce processus PDP si on ne pouvait pas dire ce que l'on pense? Je vous donne un exemple. Je ne dis pas que cela c'est le cas, mais si par exemple le président n'est pas efficace, vos idées ne peuvent pas être transmises. Je ne sais pas, on ne vous donne pas la parole, etc.

S'il y a des problèmes pendant ce PDP, l'idée c'est de nous assurer, comme je l'ai dit auparavant, c'est que vous participez à ces PDP dans de bonnes conditions. Et comme l'a dit la représentante des États-Unis, l'idée c'est d'avoir des PDP qui soient plus courts, qui puissent donner lieu à des résultats plus vite. Du point de vue gouvernemental, deux, trois ou quatre ans, plus d'un an déjà, c'est beaucoup. Je n'ai pas besoin de vous expliquer les cycles de travail des gouvernements.

Nous savons que les mandats présidentiels durent parfois quatre ans et les ministères, les ministères des Affaires étrangères ont leurs mandats pendant deux ou trois ans, un an parfois. Donc, vous voyez ce que je veux dire. Donc, désolé, l'Indonésie de vous avoir fait attendre. Vous avez la parole.

ASHWIN SASONGKO SASTROSUBROTO

Merci Nico. Alors ma question était en réalité la même question que j'avais posée tout à l'heure. Cette question de l'ISOC 27001, cette norme qui empêche l'utilisation malveillante du DNS ou en tout cas, quelle en est votre expérience? Alors je vous pose cette question pour deux raisons. Tout d'abord, l'utilisation du DNS est un vrai problème en Indonésie.

La deuxième raison, c'est que l'Indonésie, comme d'autres pays, fait partie de l'ISO IEC. Et nous avons un comité conjoint qui travaille sur cette cybersécurité, le sous-comité 27. Donc, ma proposition ici, c'est que si cette norme 27001 n'est pas suffisante pour lutter contre l'utilisation malveillante du DNS, nous devons en référer à l'ISO. Ici, nous avons notre prochaine réunion en septembre. Et dans ce cas-là, il nous faudra peut-être réviser cette norme. Parce que le processus d'élaboration des politiques dont nous avons parlé est ici pour protéger nos systèmes.

Mais si l'expérience de l'ICANN montre qu'elle n'est pas suffisante, dans ce cas-là, il faut leur dire et il faut le réviser ou réviser tout ce qui ce qui est possible de réviser. Il faut également passer à la

prochaine étape. Nico, bien sûr, vous pouvez envoyer un message à l'ISO IEC.

NICO CABALLERO Merci l'Indonésie. Et l'Inde, vous avez la parole.

SUSHIL PAL Merci beaucoup, Monsieur le Président. Merci aux panélistes et merci beaucoup à Interisle et à NetBeacon pour vos rapports. Nous sommes très heureux de soutenir cette volonté d'avoir des PDP plus rapides. J'ai quand même l'impression qu'on se concentre plus sur les symptômes que sur la cause. Oui, nous sommes ici. Nous faisons une corrélation entre les coûts très bas, les enregistrements en masse avec l'enregistrement malveillant du DNS. Mais pour moi, je continue de penser que ce sont des symptômes et non pas la cause.

Je pense que la cause ici, ce sont les politiques sur les données et l'identification, les politiques du WHOIS qui impactent notre monde physique. Nous vivons dans un monde physique bien sûr, mais nous ne savons pas forcément qui sont nos voisins. Et je pense que les noms de domaine malveillants sont présents seulement parce qu'ils ont la possibilité d'être anonyme. Et si cet anonymat n'était pas garanti, nous pourrions avoir des solutions.

Donc ce que nous pouvons faire, la seule chose que nous pouvons faire, c'est de retirer un nom de domaine quand nous nous rendons compte qu'il est malveillant. Donc je ne pense pas que

d'augmenter le coût d'un TLD à 10 $ ou même à 20 $ réduira le nombre de noms de domaine malveillants, puisque les bénéfices sont bien évidemment bien au-delà que cela. Vous l'avez dit, ils représentent 18 000 $ par minute.

Donc, nous pensons que c'est un travail à faire, bien sûr, du côté du bureau d'enregistrement, mais également du côté des titulaires de noms, et c'est un coût que les bureaux d'enregistrement devront payer. Mais je pense que nous devrions chercher de ce côté-là lorsque nous cherchons des solutions.

NICO CABALLERO Merci beaucoup à l'Inde. Il nous reste sept minutes et nous avons cette main levée. Donc je vais demander, s'il vous plaît, d'être le plus concis et clair possible. Susan est là. Est-ce que vous voulez reprendre la parole ou non? C'est bon. Alors je donne la parole à la Commission européenne, s'il vous plaît.

GEMMA CAROLILLO Gemma Carolillo pour la Commission européenne. Merci aux collègues du GAC qui ont organisé cette séance très intéressante et merci à nos panélistes. Je voulais vous référer à ce qui est demandé en termes de communiqué et de considération comme prochaine étape. De notre point de vue, c'est une très bonne chose de voir qu'il y a cette volonté.

Je pense que la plupart de la communauté souhaite avancer plus vite et plus loin sur l'atténuation des risques liés à l'utilisation du

DNS. Nous parlons des amendements des contrats. Nous avons vu de la part de la Chambre des parties contractantes des initiatives telles que celle de NetBeacon. Nous avons les résultats de l'étude d'Interisle. Donc, je crois qu'il y a un vrai momentum et il est important de prendre cette volonté de la part de toute la communauté.

De la part du GAC, notre objectif a toujours été d'avoir été de nouveaux membres avant la nouvelle série, mais il est important d'être pragmatique, d'identifier des mesures identifiables et réalisables dans le temps que nous avons. Donc cela veut dire peut-être de prioriser sans oublier la situation générale, mais peut-être de prioriser davantage. Donc il est important de réfléchir à un avis sur un PDP accéléré et peut-être plus ciblé. Mais il est également important que le GAC identifie des questions prioritaires.

Nous avons également entendu aujourd'hui la possibilité de combiner des mesures proactives comme faire le suivi des modèles et des tentatives d'enregistrement malveillants et les enregistrements en masse. C'est une très bonne proposition. Je pense qu'elle devrait être explorée et il est également important de prendre en compte les obligations de transparence. Cela faisait partie des avis du GAC, en particulier lors des amendements des contrats.

NICO CABALLERO Merci beaucoup à la Commission européenne. Je suis tout à fait d'accord. Nous avons six séances de rédaction du communiqué,

donc nous aurons le temps de nous pencher là-dessus. J'ai le Canada, les Pays-Bas, la Suisse et le Danemark.

IAN SHELDON

Merci beaucoup. Merci à tous nos panélistes, c'était très intéressant. Je vais être très bref. Merci encore et, en particulier merci à Graeme pour le rapport de NetBeacon. Je suis tout à fait d'accord avec votre point sur le fait que le mieux est l'ennemi du bien.

Il faut toujours nous concentrer sur nos PDP ciblés. C'est très important et j'exhorte vraiment les membres du GAC de lire ce rapport. Il est très intéressant, très informatif, il n'est pas trop spécifique et c'est une discussion vraiment politique. Donc encore une fois, merci beaucoup et nous avons hâte de participer aux prochaines discussions du GAC pour faire avancer ce PDP.

NICO CABALLERO

Merci. Les Pays-Bas, vous avez la parole.

MARCO HOGEWONING

Merci beaucoup. Je vous remercie également. Je voudrais remercier tous les orateurs pour cette séance très importante. Comme l'a dit mon collègue du Canada, nous pensons également que le mieux est l'ennemi du bien. Donc, nous pensons qu'il est important de réfléchir aux options qui sont disponibles et de

commencer à prioriser. Et nous espérons que nous pourrons trouver des consensus lors des prochaines réunions.

NICO CABALLERO Merci les Pays-Bas. La Suisse, vous avez la parole.

JORGE CANCIO Jorge Cancio pour la Suisse. Je me joins avec les orateurs précédents pour vous remercier. Il est très important de discuter de ces sujets avec la GNSO et avec le conseil d'administration pour voir la direction qu'il nous convient de suivre. Mais je pense qu'il est important de suivre ces PDP ciblés. Et peut-être pour aller à l'encontre de l'optimisme de Susan, je ne crois pas qu'un PDP ait déjà eu lieu en moins d'un an, mais j'ai hâte qu'on me prouve le contraire.

NICO CABALLERO Eh bien, ce sera à nous de changer cette tendance. Le Danemark, s'il vous plaît. Vous avez la parole.

FINN PETERSEN Finn Petersen pour le Danemark. Merci beaucoup, Monsieur le Président. Merci pour vos présentations à toutes et à tous. Nous sommes tout à fait d'accord sur le fait que les PDP doivent être plus ciblés. Nous voudrions qu'ils soient proposés avant le lancement de la prochaine série, donc il faudra avancer très vite. Mais nous

avons également très hâte de voir des mesures proactives mises en œuvre, en particulier pour les enregistrements.

Nous avons hâte également de voir les vérifications d'identité mises en œuvre lors de l'enregistrement ou qu'elles soient en tout cas plus exigeantes que ce qu'elles sont aujourd'hui. Bien sûr, il ne faut pas oublier des questions de transparence et c'est absolument une priorité avant la prochaine série. Donc nous devons nous concentrer sur des mesures proactives pour pouvoir avancer dans nos objectifs.

Et j'avais une question pour Interisle. Dans votre étude et dans vos considérations, est-ce que vous avez défini ce qu'était un enregistrement en masse? Quelle devrait être la limite? Quel devrait être le seuil? Est-ce que ce sont cinq enregistrements en même temps? Est-ce que vous avez un chiffre clair en tête?

GRAEME BUNTON

Graeme du NetBeacon Institute. Alors, pour les enregistrements en masse, je crois que nous avons des problèmes pour définir une limite de ce nombre de nom de domaine disponible à l'achat au même moment. Parce que dès que nous définissons un seuil, les utilisateurs malveillants en achèteront tout simplement juste un de moins que ce seuil. Définir des limites, cela impacterait également le marché et cela pourrait avoir des impacts négatifs et dangereux.

Notre objectif, lorsque nous soulevions cette question des enregistrements en masse, en particulier dans le cadre du rapport

INFERMAL, nous avons réfléchi à deux choses. La première, ce sont les API qui permettent d'avoir des outils d'accès sans spécifier comment ces outils sont utilisés.

Et le deuxième point, c'était d'avoir des vérifications de nom de domaine associées. Cela permet d'avoir une bonne réactivité possible. Mais si les bureaux d'enregistrement évaluent tous les noms de domaine dans le panier d'un client, cela aura un impact sur les bureaux d'enregistrement puisque cela leur coûte de l'argent de faire cette évaluation et cela également leur demande d'être très attentifs à qui a accès à de nombreux domaines. Et c'est pour cela que nous avons écrit dans notre rapport que cela aura un impact sur l'industrie et nous encourageons la prudence sur ces enregistrements en masse.

NICO CABALLERO Alors, pardon, nous devons absolument conclure, mais il est très rassurant de voir que nous avons un consensus ici aujourd'hui. Souvent, dans notre situation internationale, nous nous rendons compte que le consensus n'est pas toujours atteint. Donc, je suis très heureux de voir ce consensus sur une approche en ce qui concerne les considérations du communiqué sur ces questions. Je ne vais pas relire tout cela, mais en tout cas sur les avis pour la conclusion. Susan, est-ce que vous voulez rajouter quelque chose surtout parce que vous êtes la responsable thématique du PSWG?

SUSAN CHALMERS

Merci beaucoup, Monsieur le Président. Très rapidement, du point de vue des États-Unis, l'échéancier pour les PDP doit être réduit de manière significative pour pouvoir réussir nos objectifs politiques avant l'expansion du DNS. À la suite de la nouvelle série des gTLD, la dernière chose que je vous dirai pour la communauté de l'ICANN en général, c'est que nous avons entendu des propositions de NetBeacon, de la Chambre des parties contractantes.

Le Groupe des entités commerciales a également des idées. L'ALAC a également des idées, des priorités politiques. Le groupe des unités non commerciales a également offert des contributions constructives, mais nous voyons tous qu'il y a du mouvement. Nous nous dirigeons tous dans la même direction. Le modèle multipartite de l'ICANN et sa communauté doivent travailler main dans la main pour pouvoir lutter contre l'utilisation malveillante du DNS. Nous sommes à un moment charnière pour que l'ICANN atteigne ses objectifs en matière de politique. Merci beaucoup.

NICO CABALLERO

Merci beaucoup aux États-Unis. Nous allons lever la séance. Désolé, nous avons cinq minutes de retard. Vous avez 30 minutes de pause-café et juste après, nous aurons une réunion avec la GNSO et avec l'ALAC, 45 minutes chacune pour ces réunions. Puis nous aurons la pause déjeuner. Merci à toutes et à tous. La séance est levée.

[FIN DE LA TRANSCRIPTION]