ICANN78 | Réunion générale annuelle – ccNSO : point du Comité permanent sur l'utilisation malveillante du DNS
Mercredi 25 octobre 2023 – 1h30 à 03h30 HAM

CLAUDIA RUIZ : Nous allons lancer l'enregistrement.

Bonjour et bienvenue à cette séance de la ccNSO consacrée aux outils et aux mesures à propos de l'utilisation malveillante du DNS. Je suis Claudia Ruiz et je suis accompagnée de Bart Boswinkel et d'Andrea Glandon et nous allons ensemble gérer la participation des séances pour cette séance qui est enregistrée et régie par les normes de comportement attendu de l'ICANN.

Pendant la séance, les questions ou les commentaires envoyés à travers le chat ne seront lus à haute voix que s'ils suivent le format indiqué. Je lirai les questions et les commentaires à haute voix lorsque le président ou le modérateur de la séance me l'indiquera.

Le service interprétation pour la séance inclura l'anglais, l'espagnol, le français et l'arabe. Cliquez sur l'icône d'interprétation sur Zoom pour sélectionner la langue dans laquelle vous souhaitez intervenir pendant la séance.

Si vous voulez parler, levez la main dans la salle Zoom et lorsque le facilitateur de la séance vous l'indiquera, allumez votre microphone. Avant de parler, assurez-vous d'avoir sélectionné la langue dans laquelle vous allez parler à partir du menu d'interprétation. Dites votre

nom pour les registres ainsi que la langue dans laquelle vous allez parler si ce n'est pas l'anglais. Au moment d'intervenir, assurez-vous de mettre sur muet tous vos autres dispositifs et leur notification. Parlez clairement et à un rythme raisonnable afin de permettre une interprétation exacte de vos propos.

Cette séance inclut un service de transcription en direct automatisé. Veuillez noter que cette transcription n'est pas officielle et ne fait pas autorité. Pour accéder à la transcription en direct, cliquez sur le bouton Closed Captions dans la barre à outils de Zoom.

Pour garantir la transparence et la participation au modèle multipartite de l'ICANN, nous vous demandons de bien vouloir accéder aux séances de Zoom avec votre nom complet, soit prénom et nom de famille. Vous pourriez être exclu de la séance si vous n'accédez pas avec votre nom complet. Merci.

Je vais maintenant céder la parole à Nick Wenban-Smith. Merci.

NICK WENBAN-SMITH : Merci pour cette présentation. Pour ceux qui ne me connaissent pas déjà, je m'appelle Nick Wenban-Smith et je représente le ccTLD .uk. Aux fins de cet après-midi et jusqu'à ce que la communauté puisse identifier un président mieux qualifié, je préside le comité permanent de la ccNSO relatif à l'utilisation malveillante du DNS. Nous sommes toujours contents de recevoir vos contributions. Et si ce que nous présentons cet après-midi éveille votre intérêt à ces sujets, vous êtes plus que bienvenus à rejoindre notre groupe qui est composé de participants très divers. Mais bien sûr, on peut toujours accueillir plus de

participants. C'est un groupe collégien. Ce qui nous amuse le plus, c'est de discuter de ces sujets ardus que traite l'ICANN.

À l'écran, vous voyez l'ordre du jour que nous avons prévu pour aujourd'hui. J'essaierai de présider cette séance, comme je le disais avant. Et lorsqu'on met l'heure sur les diapos en UTC, je suis toujours un peu dérouté, mais à ce que j'ai compris, il s'agit d'une séance de deux heures. Ce n'est pas ce que dit la diapo. Parfois, quand on parle de l'utilisation malveillante du DNS, on ne fait pas confiance à ce qu'on voit. C'est métaphorique, vraiment, d'avoir ces heures mal exprimées.

Nous allons voir quelles sont les ressources que fournit le comité permanent consacré à l'utilisation malveillante du DNS aux ccTLD, puis nous allons voir les différents aspects des outils et des mesures dédiés à cette importante question de l'utilisation malveillante du DNS.

Finalement, je dirais qu'un de mes grands intérêts, une de mes passions, c'est de m'assurer que mon ccTLD soit sûr, tout d'abord, puis de garantir la sécurité de tous les autres ccTLD. Mais il faut que l'on reconnaisse face à la communauté que les ccTLD et les gTLD ont beaucoup de points communs au moment de mesurer et de prévenir l'abus. Il ne sert à rien que de s'occuper de son propre cloison CC sans prendre en considération les gTLD. La GNSO a d'ailleurs son propre groupe de travail sur l'abus du DNS, donc il s'avère raisonnable de les inclure dans la discussion et de débattre pour voir ce qu'on pourrait mieux faire ensemble, comment on pourrait mieux collaborer. Diapo suivante.

Un petit récapitulatif pour les nouveaux venus. La ccNSO n'élabore pas de politique pour les ccTLD dans ce domaine. Au contraire, nous avons une mission qui est limitée à l'élaboration de politiques spécifiques aux activités de l'IANA. Or, s'agissant de politiques pour les ccTLD individuels, ce n'est pas notre rôle. En tant que juriste, j'aime toujours aller voir quels sont les termes de référence et j'y consacre tout mon temps libre. Si je suis là, c'est surtout pour partager des informations avec vous, ce n'est pas pour parler de ces aspects.

On est là pour montrer des exemples de ce qui fonctionne bien pour lutter contre l'utilisation malveillante du DNS. Et parfois, quand on se réunit, on apprend et on tire des leçons de ce qui n'a pas bien marché. On se réunit pendant les pauses et on discute de tous ces cas-là moi-même. Je suis très ouvert et j'avoue très ouvertement que je fais des erreurs. Mais souvent, il est bien plus utile d'apprendre des erreurs des autres.

Ce dialogue ouvert et constructif n'est pas un mérite pour lequel je puisse réclamer que l'on me félicite, mais cela a été un groupe de travail ouvert et très collaboratif.

Finalement, pour parler d'élaboration de politique, l'idée est de donner à la politique les ressources nécessaires pour être de meilleurs gardiens de leur propre TLD. Et surtout, on vise à aider les autres à faire en sorte que l'Internet soit un endroit plus sûr et atténue l'impact de l'abus de DNS. Diapo suivante.

On a toujours les mêmes heures. Comme vous voyez, la COVID n'a toujours pas été gentille avec tous. Si vous voyez sur les photos, il y a

des gens pour qui on dirait que ça n'a pas été aussi grave. On va s'en tenir à ce commentaire, je ne vais pas aller plus loin. En tout cas, comme vous voyez, on va maintenant parler des ressources pour les ccTLD, outils, mesures et finalement, on aura un dialogue.

Je vais céder la parole à David.

DAVID MCAULEY : Merci Nick. Je suis David McAuley. Je suis employé de Verisign et je participe à la ccNSO grâce à notre gestion de codes de premier niveau géographique, des ccTLD. Je remercie mes collègues de la ccNSO de m'avoir accueilli. Je vous souhaite la bienvenue à mon tour.

Tout d'abord, je veux vous rappeler ce que nous sommes en train de faire au sein du sous-groupe du DASC que je préside, qui s'appelle le sous-groupe des services d'annuaire. Comme le disait Nick, il ne s'agit pas d'un code de comportement mais plutôt de la création d'outils de collaboration efficaces pour les gestionnaires de ccTLD pour leur permettre de répondre de manière efficace à l'utilisation malveillante du DNS.

Tout d'abord, je vais vous parler d'une initiative en cours qui est la création de notre référentiel d'informations. Je vais pour ce faire céder la parole au représentant de CIRA, le .ca, Adam.

ADAM EISNER : Merci. Comme vient de le dire notre cher ami ici à mes côtés, je travaille pour CIRA. Je voulais tout d'abord consacrer quelques minutes à vous

parler de la bibliothèque de ressources et du référentiel qu'on est en train d'élaborer ensemble au sein du DASC.

L'objectif ici est de créer un espace dédié pour que les gestionnaires de CC puissent aller chercher des ressources et partager des informations. Il s'agit d'un espace géré par un petit conseil responsable des contenus, un comité éditorial. On se réunit quelques fois par mois pour passer en revue quels sont les contenus qui ont été envoyés. Et au cours des prochaines minutes, je vais vraiment insister et vous encourager à envoyer des informations, à partager, à collaborer. Vous allez entendre dire cela très souvent lorsqu'on parle du travail qu'on est en train de faire, c'est quelque chose de tout neuf et on essaie d'encourager la collaboration autant que possible. Je dirais que c'est également le cas pour ce référentiel des informations.

Ce comité se réunit plusieurs fois par mois pour passer en revue ce qui a été contribué. L'objectif est d'avoir également un rythme périodique de documents d'information qui sont publiés. On veut avoir une périodicité pour fournir des informations et pour les recevoir à la fois. Diapo suivante.

On a différentes catégories dans ce référentiel au nombre de quatre : présentations et rapports, outils que peut utiliser la communauté, politiques et définitions, et articles et commentaires, le tout en lien avec l'utilisation malveillante du DNS. Lorsque vous allez accéder au référentiel, vous verrez que tout est divisé en ces quatre catégories. On a inclus ici un code QR pour pouvoir accéder au référentiel. Nous vous encourageons à y accéder à tout moment.

Les critères pour ce qui peut être envoyé sont très généraux, très amples. Bien sûr, le contenu doit être lié à l'utilisation malveillante du DNS et aux ccTLD. Mais ceci étant, il peut y avoir toute une série de sujets dans l'écosystème. Ce peut être une question de bureaux d'enregistrement, d'opérateurs de registre, de thèmes, de menaces ; peu importe. L'idée est de rester aussi large que possible et de ne pas trop cerner les résultats parce que l'idée est d'avoir une base de ressources qui soit utile dans ce référentiel.

Au niveau du format, on est aussi assez flexible et je pense qu'en termes généraux, tout type de format que vous consommerez pour accéder aux informations nous conviendra. L'idée est d'avoir des exigences qui ne soient pas trop difficiles. Tout type de fichier est accepté. Diapo suivante.

Je sais que cette diapo n'est pas géniale pour montrer de quoi cela a l'air, mais on a ici ajouté quelques tableaux pour montrer ce qui est déjà dans le référentiel. Vous voyez que cela varie entre entretien avec l'Institut sur l'abus du DNS, des documents qui ont été publiés lors des séances de la ccNSO aux réunions précédentes de l'ICANN et des outils, des définitions et autres. On a une large gamme de types de contenus qui parlent aux différents publics de différents sujets. Nous allons continuer à essayer de pouvoir compléter cette base de catégories à partir de ce que nous avons déjà. Diapo suivante.

Finalement, quant au processus, c'est assez simple, direct. On n'a pas beaucoup de technologies. On prend les présentations qui sont envoyées à une adresse e-mail spécifique qui est celle qui apparaît à l'écran. Plus vous nous fournirez des informations, plus on vous sera

reconnaissant au moment de recevoir ces documents et ces informations. Vous voyez ce qu'on cherche au moment de recevoir ces contributions. Pour nous aider à mieux savoir comment classer le contenu que vous partagez, nous avons ajouté ici différents champs. Et dans le délai de quelques semaines d'avoir reçu une contribution, le groupe passera en revue le matériel, tout d'abord individuellement, et nous nous mettrons d'accord et déciderons sur la base du consensus de ce qui doit être publié sur le référentiel et ce qui ne le sera pas. Comme je l'ai déjà dit à plusieurs reprises, on accepte tout, vraiment. On veut vraiment recevoir les contributions de la communauté.

Finalement, c'est une nouveauté qui a été lancée lors de la réunion précédente de l'ICANN. On commence à peine à travailler. Et je vais céder la parole à David qui va vous parler d'une de nos autres initiatives à travers la liste de diffusion et d'e-mails. Merci.

DAVID MCAULEY : Comme vous voyez sur la ligne chronologique qui apparaît à l'écran, lors de l'ICANN78, l'idée était d'annoncer une liste de diffusion par courrier électronique. On n'y est pas parvenu. On est en train d'élaborer et de développer un outil de contact par e-mail dont je vous parlerai pendant quelques minutes. Le travail a été complété, mais il n'a pas été approuvé et ce ne sera qu'à la fin de cette réunion que nous passerons par cette approbation. Ce sera un processus très rapide, suite auquel nous ferons une annonce à la communauté par rapport à cette liste de contacts et de diffusion. Normalement, ce devrait se faire dans le prochain mois.

Notre collègue Fernando Espana de .us devait faire cette présentation. Malheureusement, il est tombé malade. Je le remplace par conséquent. Une liste de diffusion dédiée, quelques paramètres. Comme je l'ai dit, ceci sera inspiré de l'*Ops list* des TLD. Il s'agit d'une liste de diffusion fermée par e-mail pour les gestionnaires de ccTLD. Bien sûr, comme ce sont des e-mails, nous ne pouvons pas garantir la confidentialité car ils peuvent être renvoyés. Le TLD Ops est un outil très utile et adapté aussi aux questions de sécurité. L'idée est de partager des informations, d'envoyer régulièrement des données de contact et de permettre des conversations hors ligne ou hors liste en fonction des besoins et des expériences de chacun.

Chaque ccTLD bénéficiera de quatre inscriptions pour des personnes de leur groupe. Vous pouvez avoir trois personnes nommées et un rôle nommé, en général des personnes plutôt du profil technique, juridique ou opérationnel. C'est finalement assez semblable au référentiel lui-même. L'idée est de favoriser la collaboration sur les questions d'utilisation malveillante du DNS. Vous trouverez ici des informations sur ce projet. C'est encore un peu prématuré puisque cette information sera diffusée dans notre annonce. Vous pouvez noter les informations de cette diapositive, mais elle vous parviendra également par le biais de l'annonce. La suivante, s'il vous plaît.

Ensuite, il y a des informations sur la façon de s'inscrire. Je pense que vous ne pouvez peut-être pas la voir, mais c'est très simple. Vous vous inscrivez tout simplement à la liste de diffusion et nous vous enverrons des notes par rapport à la nature de la liste, comment elle fonctionne, quels sont les critères de sélection, etc. Voici l'équipe qui est très

réduite de six personnes : Fernando Espana, Jordi, Adam, Diego, Mary et moi-même. Nous sommes là pour répondre aux besoins de la communauté et aux besoins des gestionnaires de ccTLD.

Une fois ces outils de collaboration lancés, nous vous invitons à les utiliser de la façon qui a été décrite par Adam. Si vous êtes intéressé, inscrivez-vous, examinez la liste de diffusion et nous pouvons l'utiliser de plusieurs façons. Ce sont des données d'information qui seront disponibles en fonction de vos besoins. La suivante, s'il vous plaît.

Nick, je vous redonne la parole.

NICK WENBAN-SMITH : Merci David et merci aux collègues pour ce travail.

Le point suivant, c'est la partie centrale concernant les outils et les mesures. Quatre présentations. Une observation : nous essayons tous de mesurer la même chose. Alors, pourquoi avoir des outils de mesure différents et envoyer des messages contradictoires concernant la gestion de l'utilisation malveillante du DNS ? Nous allons avoir des perspectives très intéressantes. Passons à la diapositive suivante.

L'enquête que nous avons faite au quatrième trimestre de l'année 2022 posait une question très simple, sur une base d'auto-évaluation, bien sûr, nous savons que la définition de l'utilisation malveillante peut varier et il y a peut-être certaines restrictions aux réponses qui ont été fournies par les participants, mais ce qui est au moins clair et qui n'est d'ailleurs pas une surprise, c'est que les ccTLD participants ont des niveaux d'utilisation malveillante très bas, ce qui confirme nos

intuitions. Ce qui est intéressant à droite, c'est que 38 % des personnes qui ont répondu à cette enquête indiquent qu'ils ne sont pas tout à fait certains du volume d'utilisation malveillante du DNS dans leur ccTLD. Bien sûr, si l'on est un gestionnaire de ccTLD « responsable », c'est une information qu'il faudrait savoir. C'est là tout l'objectif de cette session, de vous donner plus d'informations et plus d'outils sur la question.

La difficulté, bien sûr, c'est qu'il n'y a pas une formule magique. C'est un travail minutieux et de détail. Nous espérons réaliser à nouveau cette enquête au quatrième trimestre de 2024 pour voir si peut-être la situation a évolué positivement puisqu'il est important que les ccTLD connaissent de façon claire les niveaux d'utilisation malveillante dont leurs ccTLD sont victimes.

Pour mettre tout le monde à la page, cette citation est importante. Une gestion de ccTLD sécurisée pour le bénéfice d'une communauté passe par un contrôle et une mesure. Je connaissais cette citation, elle est apparemment attribuée à Peter Drucker. Mais l'essentiel, c'est le message : ce qui ne peut pas être mesuré ne peut pas être géré ou contrôlé. C'est pourquoi la connaissance des niveaux d'utilisation malveillante ou d'abus du DNS est importante. Cela vous permettra également de mesurer l'effet des mesures que vous adopterez. Bien sûr, pour pouvoir mesurer, il faut savoir de quoi on parle.

Je voulais aussi vous présenter mon expérimentation psychologique favorite. Hawthorne, c'est un consultant spécialisé et il s'est intéressé à la question de la productivité en fonction du niveau de lumière. Ils se sont rendu compte qu'en changeant les ampoules, les travailleurs étaient plus ou moins efficaces. L'une des choses intéressantes qu'ils

ont trouvées, c'est que même s'ils ne changeaient pas les ampoules, les personnes qui participaient à l'expérience, tous sans exception, avec de nouvelles ampoules ou pas, devenaient plus productifs. Il en retourne en fait que les personnes qui se savent mesurées, qui se savent suivies dans leurs pratiques, deviennent plus productives. Le fait de mesurer les choses modifie le comportement des personnes qui font l'objet de cette mesure. Je crois que c'est quelque chose qu'il faut prendre en compte.

Passons à la diapositive suivante puisque celle-ci n'est qu'un résumé. Je donne la parole à Rowena.

ROWENA SCHOO : Merci beaucoup à la ccNSO de nous avoir invités aujourd'hui. La suivante s'il vous plaît.

Quelques mots d'introduction concernant l'institut, ensuite la mesure de l'utilisation malveillante du DNS., ensuite notre projet qui s'appelle Compass ou la boussole, quelques-uns des défis auxquels nous faisons face et la situation actuelle.

L'Institut sur l'utilisation malveillante du DNS a été créé par PIR dans le cadre de sa mission sans but lucratif. L'idée est de mieux connaître le phénomène pour défendre l'intérêt public. Nous parlons lorsque nous parlons d'utilisation malveillante d'utilisation malveillante technique comme l'hameçonnage, le pharming, les logiciels malveillants, les botnets et le spam. L'idée est d'identifier les points les plus complexes qui ont été identifiés par la communauté et essayer d'y proposer des solutions pour la communauté dans son ensemble.

Nous couvrons tous les TLD et tous les bureaux d'enregistrement. Tout ce que nous faisons est gratuit, donc je ne suis pas là pour vous vendre quoi que ce soit aujourd'hui. Nous présentons plutôt des ressources gratuites qui sont utilisables pour votre compréhension de l'utilisation malveillante du DNS. Nous avons également un conseil consultatif et Nick et Bruce sont les représentants du ccTLD.

Lorsque l'on mesure l'utilisation malveillante du DNS, on applique en général ce pas-à-pas que vous voyez à l'écran. Quel est l'objectif ? Quelle est l'approche ? La plupart de ces études prennent des informations provenant des listes de réputation et de blocage. Il y en a des centaines, voire des milliers de niveaux de qualité variables et en général, elles ne sont pas assorties de preuves.

L'étape suivante requiert par conséquent une sorte de nettoyage et si l'on est intéressé par des domaines uniques par exemple, l'idée est de réduire cette liste d'URL à une liste de noms de domaine. Parfois, ce sont des adresses IP aussi, donc il faut savoir ce que l'on veut mesurer. Il est important de savoir qu'il n'existe aucune liste qui n'ait pas de faux positif. Il est important de prendre cela en compte dans les études. Ensuite, en fonction des objectifs, il y a plusieurs niveaux d'analyse et des décisions ensuite sont prises par rapport à la présentation des données. Ce sont des décisions difficiles qui doivent être prises pendant tout ce processus et ceci peut avoir une influence sur les chiffres et les résultats.

Je voulais vous parler aussi de notre projet que l'on appelle Compass, la boussole. Lorsque nous avons ouvert l'institut, nous souhaitions parvenir à une compréhension très approfondie de l'utilisation

malveillante du DNS. Nous souhaitions diffuser cette information au sein de la communauté pour que chacun sache ce qu'il se passe dans sa zone respective. Nous souhaitons que cette information soit aussi ventilée que possible pour être précis et surtout disposer de données comparables. Nous souhaitions également proposer des documents, de meilleures pratiques afinde réduire l'utilisation malveillante du DNS en général, nos principes sont la transparence, la crédibilité, l'indépendance, la précision et la fiabilité.

La manière de procéder était d'engager un chercheur indépendant, le docteur Maciej Korczynski, qui nous accompagne ici dans cette salle était le chercheur que nous avons engagé. Il est chercheur à l'université de Grenoble et il gère ce que l'on appelle KOR Labs, un laboratoire de l'université. Nous avons travaillé avec lui pour pouvoir justement générer cette analyse technique sur laquelle s'étaye Compass.

Au moment d'évaluer les données, on a des précisions à faire. D'une part, on ne mesure pas tout ce qui est nuisible sur Internet, pas tout ce qu'il y a de mal. Au contraire, on cherche à avoir de l'exactitude et de la fiabilité par-dessus l'exhaustivité, et ce, pour pouvoir avoir des références dans l'écosystème et dans la durée.

Une autre décision que nous avons prise, c'était qui nous intéressait non pas de savoir combien d'abus il y avait mais si cet abus avait été atténué. L'atténuation était vraiment importante pour nous dans ce projet.

Par ailleurs, on voulait comprendre quels étaient les types d'enregistrement qui étaient des victimes d'abus, c'est-à-dire si un nom

de domaine était enregistré aux fins d'une utilisation malveillante ou si c'était accidentel. On a dû faire des compromis pour pouvoir obtenir ces informations et en général, ce qu'on voit est que les domaines abusés sont compromis, c'est-à-dire qu'ils ne sont pas enregistrés à des fins malveillantes d'emblée. Il est important de comprendre tout cela au moment de décider des mesures d'atténuation à entreprendre et comprendre les dommages collatéraux.

Ici, vous voyez visuellement ce que j'étais en train d'expliquer verbalement pour les segments spécifiques et surtout ce qui peut être nuisible. On peut tous signaler ce qui peut être nuisible, tout ce qui ne l'est pas. Parfois, on parle de cela comme du principe de l'iceberg parce qu'on ne voit qu'une petite pointe et il y a énormément plus de masse au-dessous de l'eau. On voit les dommages, on ne voit pas tout ce qu'il y a avant. La décision était de nous concentrer spécifiquement sur le logiciel malveillant et sur l'hameçonnage. On a concentré nos efforts sur les preuves fiables pour ces deux types d'attaques.

Je vous demande d'être bienveillants lorsque je montre ce schéma, je sais qu'il est compliqué, mais c'est une représentation visuelle de notre méthodologie et de ce qui est sur notre site Web. C'est ce qui vous permettra de comprendre comment nous sommes parvenus à avoir les mesures que nous avons. Comme je le disais à l'instant, ce type de processus reprend le travail pionnier d'autres projets, comme le DAAR qui date d'il y a quelques années. Pour nous, il était très utile d'utiliser leur contribution. On a travaillé avec PhishTank, OpenPhis et URLHaus. On est passé par le processus de nettoyage de données. Je tiens à préciser ici autre chose d'important qui est le fait de comprendre que

certaines de ces listes ont 70 000 URL ou plus, et ce, parce que certaines attaques génèrent la création de nouveaux URL, que ce soit des attaques robotisées ou humaines.

Par ailleurs, on a des noms de domaine qui sont compris comme domaines spéciaux. C'est ce type de domaine qu'a supprimé KOR Labs, par exemple les services de raccourcissement d'URL. D'autres comme docs.google.com sont des services de partage de fichiers qui étaient également ciblés. L'idée est de faire en sorte que cette liste de domaines spéciaux soit publiquement disponible pour que tout le monde puisse nous aider à mettre à jour cela.

D'autre part, on avait l'analyse, la collecte de preuves, les captures d'écran, les registres DNS, etc. À ce moment-là, on décidera si le nom de domaine était enregistré à des fins malveillantes où il a été compromis. KOR Labs va visiter le site Web pour comprendre si cette décision est correcte ou pas. On va voir quels sont les attributs qui ont été pris en compte et on verra à quel moment du processus intervient la mesure d'atténuation, si cela prend cinq minutes, 15, 30, après dans les délais d'heures entre une et six heures et puis les jours, on prend des mesures toutes les douze heures pendant 30 jours pour voir si ces mesures d'atténuation continue à intervenir.

Puis, on publie des rapports. Par exemple, on publie des rapports mensuels où on inclut les abus tous les 100 000 domaines sous gestion avant de décider. Mais sur ces données, il y a des exclusions. Par exemple, si on a des niveaux très faibles d'hameçonnage et de logiciels malveillants qui ont été identifiés pour ce mois-là, vous serez exclus de

la liste des faux positifs et on ne se concentrera que sur les enregistrements à des fins malveillantes. Diapo suivante.

Au moment de mesurer les données, il existe des difficultés qui sont communes à tous les projets sachant que toutes les mesures suivent les essais de faire de notre mieux. Mais il y a des problèmes de faux positifs. Il y a un blog qui sera d'ailleurs très prochainement publié où nous parlons de ce type de difficultés. Les simulations d'hameçonnage sont très similaires aux cas d'hameçonnage pour le monde extérieur. Parfois, on finit par être dans des listes de blocage. On semblerait répliquer le problème. Avec les données, le problème qu'on a est que très souvent, elles sont biaisées, elles sont distribuées largement et ce peut être difficile lorsqu'on parle de petits chiffres, surtout dans le cas de ccTLD, parce qu'on n'a pas suffisamment de résultats.

On a également le problème de savoir qu'il y a des biais géographiques, dans la langue et autres. Puis, on a également la taille des zones et les nouveaux enregistrements dans le cadre des ccTLD, ce qu'on essaie de résoudre. C'est pour cela qu'on dit que tous les ccTLD peuvent participer.

J'ai inclus ici énormément d'informations. Si vous voulez relire les diapos, vous pourrez le faire, mais l'une des décisions que nous avons prises au moment d'élaborer des rapports est qu'on ne fait pas de moyenne de cas d'abus sur 12 mois ; au contraire, on a un processus de réduction. Si vous avez des niveaux élevés de cas d'abus tous les 100 000 domaines sous gestion et que vous apparaissez dans un de nos tableaux mais seulement pour un mois, on ne publie pas votre TLD. Vos données seront expurgées, et cela, parce que si vous êtes un TLD tout

petit comme celui de l'exemple et que vous êtes la cible d'une attaque malveillante pendant un mois, vous atténuez le tout. Mais vous pourriez quand même avoir un taux d'abus assez élevé tous les 100 000 domaines sous gestion, parce que vous avez un petit TLD. Mais ce n'est pas correct et ce n'est pas exact non plus par rapport à ce qui se passe au sein de ce TLD.

Encore une fois, que devrait faire un ccTLD à partir de ces informations ? Vous devez réfléchir à votre objectif. Interrogez-vous par rapport à la manière dont ces chiffres sont générés. Quels sont les résultats ? Sachez qu'il y a des faux positifs, cela arrive. Finalement, aidez-nous à améliorer la qualité de ces données. On voudrait connaître votre avis. On a des tableaux de bord gratuits pour chaque TLD, pour chaque bureau d'enregistrement. Venez nous voir, on pourra vous présenter tout cela dans les détails pour vous aider à comprendre les chiffres. Cette semaine même, nous avons lancé l'accès à ce système avec des crédentiels pour que vous puissiez accéder et vérifier ces informations à tout moment. On est vraiment des gens agréables. On aime bien notre travail, on veut l'améliorer, on veut avoir de meilleures données. Vraiment, venez nous voir.

Voici le tableau de bord pour le .org. Le PIR nous a très aimablement permis de montrer ces chiffres. Ils ont des chiffres d'abus pour hameçonnage et logiciel malveillant sur la gauche. Comme vous voyez, ce résultat n'est plus le même ; ils ont réduit la quantité de cas d'abus pour tous les domaines qu'ils ont sous gestion. Ici, on a une ventilation des données, les cas d'abus sur la gauche et l'atténuation sur la droite.

Je pense avoir tout dit. Merci. Si vous avez des questions, venez nous voir. On a déjà fait une présentation lors de la journée technique d'avant-hier également. Si vous n'étiez pas là, je vous encourage à aller chercher l'enregistrement.

NICK WENBAN-SMITH : Merci Rowena, on va garder votre présentation. Je pense que le mieux est de permettre à tous de présenter et de voir quelles sont les questions dans la salle. Sauf s'il y a des objections tout de suite, je pense que c'est comme cela qu'on va procéder.

On a maintenant Nathan Alan de la fédération de recherche DNS qui va intervenir.

NATHAN ALAN : Merci. C'est un plaisir d'être ici, parmi vous aujourd'hui. Je suis là pour parler de qui nous sommes en tant que DNS Research Federation, fédération de recherche sur le DNS. Notre travail au niveau des ccTLD, je vais vous présenter une vue d'ensemble et à partir de ce moment-là, on verra comment avancer.

Je disais que nous sommes une organisation à but non lucratif du Royaume-Uni. Notre objectif est de promouvoir la compréhension de l'impact du système des noms de domaine sur la cybersécurité, la politique et les normes techniques, ce que nous faisons de différentes manières, entre autres à travers notre aide sur la formation et les recherches au niveau du DNS. Nous aimons aider les personnes avec lesquelles nous discutons, on leur donne l'accès à des données à

travers la création de notre propre plateforme d'analyse dont je vous parlerai un peu aujourd'hui et finalement, nous aimons participer à l'élaboration des normes techniques pour essayer de comprendre quelles sont les normes qui sont proposées et comment nous pouvons aider à les améliorer.

Voici notre site Web. Vous voyez ici quelques-uns des projets de recherche auxquels nous avons participé récemment. Nous allons aujourd'hui parler un peu de la table de TD lorsqu'on abordera les niveaux d'abus entre les différents types de TLD. Mais nous avons également des projets de recherche en lien avec les normes Internet et la mesure d'adoption du RPKI. Finalement, nous avons également récemment entrepris des études sur les blockchains.

Le rapport que nous avons récemment publié, c'était plus tôt dans l'année, été publié à l'intention de la BC de l'ICANN qui nous avait demandé de nous pencher spécifiquement sur les taux d'abus pour les ccTLD européens. Notre idée était de trouver une manière de pouvoir classer chacun des différents TLD européens, mais également tous les ccTLD, les gTLD, les TLD clés hérités et historiques. Nous avons adopté une méthodologie de très haut niveau avec différents ensembles de données qui étaient disponibles sur notre plateforme. Mais pour chacun des rapports que nous avons vus pour un nom de domaine en particulier, ce nom de domaine a été comptabilisé une fois. Je précise cela parce qu'il est important dans cette mesure du fait qu'on voulait créer des taux qui puissent être comparables sur un même marché pour un même nom de domaine qui agirait toujours comme un seul résultat.

À la fin, cela a été divisé par la taille d'enregistrement du TLD pour nous donner le résultat du taux d'abus pour ce TLD.

Comme vous l'avez entendu dire, nos données montraient que ces ccTLD avaient des niveaux d'abus moins élevé. Et les ccTLD européens étaient ceux qui avaient les taux d'abus les plus faibles. C'est ce qu'ont montré les études. On voulait finalement comprendre quels étaient les TLD qui étaient en haut dans la liste, qui étaient ceux qui souffraient le moins de ces cas d'abus, qui étaient le moins victimes. On voulait comprendre ce qu'ils étaient en train de faire et pourquoi ils avaient ces résultats qui dépassaient ceux des autres.

Encore une fois, j'ai inclus une capture d'écran de notre site Web. N'hésitez pas à y entrer, à aller regarder nos recherches, cherchez les données qui sont présentées. Nous sommes ici à l'ICANN avec un stand également. Si vous voulez avoir plus de détails pour savoir comment nous avons pu générer et calculer certains de ces taux, comment nous avons tiré certaines des conclusions que nous présentons, nous vous expliquerons tout cela avec grand plaisir, venez nous voir.

Le rapport, qui porte surtout principalement sur les ccTLD européens puisque c'était l'objectif de notre étude, montrait que les ccTLD européens étaient moins abusés. Mais il n'y avait pas de solution clé ou de panacée pour laquelle ils avaient des niveaux d'abus moins élevés. Ils étaient tous rétroactifs au niveau de leurs approches et ne prenaient pas en considération les cas d'abus qu'on avait vus dans toutes les données qu'on avait collectées. Mais ils suivaient également les orientations d'une étude de CENTR qui aide à comprendre quelles étaient les mesures que prenaient ces ccTLD, pour comprendre leurs

clients, pour vérifier quelles étaient les lacunes, les données des titulaires de noms de domaine, pour les comprendre, pour s'assurer que les données soient correctes et exactes. Comme je le dis, il y a eu différentes mesures qui ont été prises. Ce n'était pas une seule mesure qui ait été adoptée pour atténuer l'utilisation malveillante du DNS. Encore une fois, vous voyez ici où trouver les liens pour accéder à ce rapport que j'évoque. Je pense que c'est tout de mon côté, si je ne me trompe.

Ici, une fois encore, une vue du tableau que nous avons créé. Les rapports sont rangés par nom de domaine et par nom de l'hôte. Ceci est à peine une petite image et nous pouvons vous en donner une démonstration plus en détail si vous en avez besoin. Quelques liens vers certaines sources qui pourraient vous intéresser que j'aie mentionnées aujourd'hui.

Voilà, c'est tout pour moi.

NICK WENBAN-SMITH : Merci beaucoup, Nathan. Je crois que ces trois ressources seront sans doute très utiles pour les personnes ici présentes qui souhaitent mesurer l'abus du DNS.

Maintenant, nous avons Samaneh. Je crois que je vais l'appeler par son prénom seulement, vous comprendrez pourquoi. Une approche un peu différente concernant la mesure de l'utilisation malveillante du DNS. Samaneh, c'est à vous.

SAMANEH TAJALIZADEHKHOOB : Bonjour, je suis Samaneh, j'appartiens à l'équipe de sécurité, de résilience de l'ICANN. Je prendrai la parole avec mon collègue Siôn Lloyd. Cette présentation est un peu différente des présentations habituelles de l'ICANN. Nous commençons par présenter les chercheurs de la communauté et ce qu'ils essaient de faire en matière d'utilisation malveillante du DNS.

Cet abus du DNS est mesuré en général par la création de différents indicateurs. Pourquoi ces indicateurs sont importants ? Et pourquoi essayons-nous d'en améliorer constamment la qualité ? Sur cette diapositive, vous verrez deux batteries de données. Le graphique de gauche montre les chiffres bruts à gauche et les pourcentages à droite. La perspective est très différente en fonction de l'organisation des données et des indicateurs ; les mêmes données peuvent être présentées de différentes manières et les conclusions s'en verront donc modifiées également. C'est pourquoi il est très important de veiller à la qualité de la création de ces indicateurs et à la façon dont nous présentons ces données. Plus les données sont bonnes, sont propres, sont libres de faux positifs, plus l'analyse sera précise. Parce qu'en général, surtout lorsque l'on parle des RBL, il y a très peu de données sans faux positifs. Donc, le nettoyage de ces données est très important.

Ensuite, il peut y avoir des définitions plus précises de ce que nous mesurons. Très souvent, le spam est considéré soit comme l'e-mail que l'on reçoit, l'indésirable, soit le mécanisme d'envoi de ces messages. La définition a un impact sur les statistiques. Il y a également des erreurs d'incorporation des mesures, par exemple ce que les données que nous utilisons représentent ou ne représentent pas. Par exemple, si on

montre un graphique à point à la communauté, il faut bien rappeler que l'on montre un phénomène sans pouvoir néanmoins en expliquer directement les raisons. La suivante, s'il vous plaît.

Qui sommes-nous dans l'ICANN ? Nous sommes le groupe de recherche sur la sécurité, la stabilité et la résilience de l'ICANN. Nous sommes un centre de réflexion, si vous voulez, et nous menons à bien des recherches concernant la sécurité des identificateurs de l'Internet. Notre objectif est d'améliorer la fiabilité des indicateurs. Nous en créons de nouveaux ou nous améliorons les indicateurs existants et le cœur de notre travail est d'utiliser des données et des méthodes scientifiques pour répondre aux questions qui intéressent notre communauté.

Ceci est une vue d'ensemble du travail de notre groupe. L'objectif principal est d'améliorer les indicateurs de sécurité dans le domaine des identificateurs de l'Internet, qui est le carré noir en bas à droite. Nous utilisons pour cela des indicateurs et il y a différents projets sur lesquels nous travaillons. Les données que nous collectons proviennent de différents lieux, des RBL, des fichiers de zone, etc. Nous établissons des indicateurs et nous prenons des mesures. Par exemple si nous parlons de listes de réputation et de blocage, nous créons des méthodes pour évaluer les listes RBL que nous utilisons et qui sont utilisées aussi par les membres de la communauté, les membres de ce panel.

En ce qui concerne les fichiers de zone, nous avons des méthodes pour représenter les espaces de nom de domaine qui sont actifs ou inactifs.

Dans l'article que nous avons publié cette année, près de 20 % des zones peuvent être des domaines non actifs.

Ensuite, nous avons également des projets qui utilisent des données qui ont été rapportées, comme des courriels indésirables. Nous avons également travaillé sur des outils de classement. En ce qui concerne les mesures de l'abus, nous avons le projet DAAR qui est le signalement des cas d'utilisation malveillante des noms de domaine – je sais que vous le connaissez ici toutes et tous. Nous avons des projets qui mesurent le temps en ligne de ces sites Internet marqués par une utilisation malveillante.

Je vais maintenant vous parler du DAAR, donc des outils de signalement des cas d'utilisation malveillante des noms de domaine. Nous savons que certains ccTLD participent à ce projet. Quelques mots là-dessus.

Vous le savez déjà, le projet DAAR rassemble des données de différentes RBL au niveau des TLD et les combine avec un comptage des domaines du fichier de zone. Ce projet est en vigueur depuis octobre 2017. Les TLD ont accès à leurs statistiques d'abus par le biais des API disponibles à cet effet. Ces outils peuvent également créer des séries temporelles plus longues en fonction des besoins d'analyse.

Voici les ccTLD qui se sont portés volontaires pour participer à ce projet. Nous remercions les ccTLD qui se sont manifestés pour tous les retours d'expérience que nous avons reçus en ce qui concerne les ccTLD, en plus des statistiques quotidiennes reçues par l'API. Il y a également un rapport spécifique aux ccTLD. La suivante, s'il vous plaît.

Voici ici un exemple du type de données qui sont présentées dans le rapport mensuel. Pour cette présentation, j'ai anonymisé les données. Il y a un .cc qui n'est ici qu'un exemple, ce n'est pas attribué à un ccTLD en particulier. Ces statistiques montrent la proportion de distribution des quatre types de données que nous utilisons. Il semble que le spam en tant que mécanisme délibéré est beaucoup plus concentré dans le domaine des gTLD que vous voyez à gauche que dans le domaine des ccTLD qui est à droite. La suivante, s'il vous plaît.

Le rapport ccTLD sur mesure qui est envoyé aux points de contact technique de chaque ccTLD. Vous pouvez voir ici qu'il y a un point bleu .cc qui est un ccTLD quelconque. Le point permet à chaque participant de s'identifier et de se positionner par rapport aux autres. Chacun peut par conséquent évaluer sa performance en matière d'abus du DNS dans les différents critères que nous surveillons.

Un autre exemple de graphique présenté dans les rapports qui sont envoyés aux gestionnaires de ccTLD. Chaque ccTLD peut se comparer à ses pairs. Vous voyez ici une série temporelle qui montre la tendance de l'abus d'octobre 2022 à septembre 2023. Comme vous le voyez, il y a des différences en matière de concentration et de manifestation des abus.

La précision et la fiabilité de nos données dépendent des indicateurs de base que nous avons, et en particulier le nombre de points de données. Pour l'espace de gTLD, le nombre de points de données, c'est-à-dire le nombre de gTLD que nous avons dans notre base de données est bien supérieur au nombre de ccTLD puisque nos données concernant les ccTLD sont limitées aux ccTLD qui se sont portées volontaires. Plus

nous avons de ccTLD, plus les statistiques et les graphiques que nous présentons seront utiles et précis.

Voici ce que le projet peut faire et ce qu'il ne peut pas faire. En sa forme actuelle, le projet ne peut pas informer d'autres niveaux que le TLD, c'est-à-dire qu'on n'a pas de mesures de domaines ni de bureaux d'enregistrement. On peut créer des analyses historiques des menaces à la sécurité et aider les opérateurs à comprendre quelle est leur situation par rapport au reste de l'espace, mais étant donné que les données sont anonymisées et consolidées, on ne peut pas signaler des domaines spécifiques qui apparaissent dans la liste et on n'a pas de classement de concentration de sécurité à présent.

Pourquoi les ccTLD seraient-ils intéressés à se joindre au DAAR ? Étant donné que vous êtes un public de ccTLD, que nous avons des ccTLD qui participent de manière très active, je tiens à préciser cela. Tout d'abord, les rapports que nous envoyons aux ccTLD leur permettront de se comparer à leurs pairs, de savoir quelle est leur position vis-à-vis des autres même sans voir les chiffres exacts, mais ils pourront déjà savoir quelle est leur performance mensuelle. En même temps, cela nous aidera à vous donner de meilleures mesures si nous avons plus de ccTLD. Les mesures que nous avons seront plus exactes. À travers votre participation au programme, vous pourrez nous faire part de vos retours. Et nous allons modifier les rapports. Jusqu'à présent, nous avons toujours adopté nos rapports à partir des commentaires que nous avons reçus ; vous pourrez avoir une influence sur la manière dont nous affichons les données pour que vous receviez des résultats qui vous conviennent mieux, qui soient plus agréables pour vous à lire. Et

vous recevrez également les rapports mensuels que nous élaborons pour votre propre suivi interne.

Qu'est-ce qui est à venir ? Prochaines étapes. L'équipe DAAR sera dirigée par une de mes collègues, Sion Lloyd, et il travaille d'ores et déjà à la création d'une prochaine version de ce rapport. Cela fait déjà presque un an qu'on travaille au confinement des exigences et des spécifications de ce projet. Dans les deux prochaines diapos. Je vais vous parler de ce que nous allons faire pour faire évoluer ce projet. Est-ce qu'on peut passer à la diapo suivante ? Je crois qu'il y a une erreur au niveau de cette présentation. Peu importe.

La prochaine version sera une plateforme de mesures. Il s'agira d'une version en modules, ce qui veut dire que de temps à autre, on divulguera de nouveaux modules qui viendront ajouter d'autres fonctionnalités. Le premier module inclura ce que fait le DAAR actuel, ainsi que des indicateurs et statistiques des bureaux d'enregistrement. Ce prochain module qui sera à peu près lancé d'ici neuf mois un an inclura des mesures pour les opérateurs d'enregistrer et pour les bureaux d'enregistrement. Il y aura un tableau de bord dynamique qui permettra aux utilisateurs de voir des données au niveau des domaines ainsi qu'au niveau des bureaux d'enregistrement et des titulaires de nom de domaine. Vous pouvez faire des recherches, voir des graphiques. Les chercheurs vont pouvoir télécharger les données si besoin. S'ils souhaitent utiliser les données en dehors du tableau de bord Web que nous proposons, ce sera possible.

Voici d'autres plans que nous avons sur le long terme pour ce projet. Bien sûr, on voudrait avoir plus de ccTLD qui participent pour connaître

ce qui leur serait plus utile. Mais dans les modules futurs, non pas dans le module 1 mais dans d'autres, nous voudrions également pouvoir inclure des mesures sur le temps qui passe entre l'enregistrement d'un nom de domaine pour des fins malveillantes et des activités malveillantes jusqu'à l'usage malveillant de ce domaine et jusqu'à l'adoption de mesures d'atténuation. Puis, on verra les mesures prédictives également nous permettant d'agir de manière préalable et préventive.

Voici les plans pour l'avenir. Encore une fois, l'idée de demander aux ccTLD intéressés ou qui ont des questions de venir nous voir. Contactez-nous, faites-nous parvenir vos retours. Si vous souhaitez participer, vous pouvez le faire. J'ai une autre diapo qui ne s'affiche pas qui contient toutes les informations nécessaires. Vous pouvez venir me voir après à la fin pour que je vous passe toutes ces informations.

NICK WENBAN-SMITH : Merci beaucoup, Samaneh. On a ici une perspective quelque peu différente, mais je pense que les ccTLD doivent adhérer au DAAR. J'espère que la plupart de ccTLD le feront à un moment ou un autre. Mais l'idée ici est de montrer que vous avez d'autres manières de trouver ces données dans des sources différentes.

Nous voyons la présentation finale de cette partie sur les mesures. On a ici des informations spécifiques aux ccTLD qui est un peu différente mais tout aussi intéressante. Il s'agit de la collaboration entre l'opérateur de registre de .nl SIDN et du ccTLD .de, DNS Belgium. Allez-y.

THIJS VAN DEN HOUT : Merci. Est-ce qu'on attend les diapos ? Non. Je commencerai par me présenter. Je suis Thijs van den Jout, je suis chercheur au sein de SIDN Labs, qui est l'équipe de recherche du registre .nl. À mes côtés, j'ai Ronald Geens, chercheur du .be de DNS Belgium et on présentera la collaboration entre nos deux registres pour essayer d'identifier les enregistrements des activités malveillantes.

Aujourd'hui, nous parlerons de différentes questions. Tout d'abord, nous présenterons le projet RegCheck qui est le projet autour duquel nous sommes en train de collaborer. Il s'agit d'une application qui permet d'avoir un processus d'apprentissage à la machine pour générer ces connaissances. Puis, nous verrons quelle a été notre approche entre le moment de l'enregistrement et de ce qui suit, comment nous avons mis en œuvre RegCheck. Ronald parlera après de leur manière de gérer les enregistrements au .be jusqu'à maintenant et ce qu'ils feront à l'avenir. Puis, nous parlerons de nos collaborations en davantage de détails et pour conclure, nous présenterons quelles ont été les leçons apprises à ce jour.

Voici RegCheck. Comme je le disais avant, il s'agit d'une application d'apprentissage à la machine pour identifier les domaines malveillants au moment de leur enregistrement. J'ai déjà présenté cela il y a quelques jours. Si vous y étiez, je vais répéter les mêmes informations. Et s'il manque des informations que j'ai présentées il y a quelques jours, vous pourrez aller chercher l'enregistrement de ma première présentation.

Vous voyez ici que RegCheck check consiste en différentes composantes techniques, à savoir tout d'abord une connexion avec les enregistrements, ce qui fait que les enregistrements sont directement informés à l'application de RegCheck. On a une base de données où on fait un suivi avec des étiquettes et on fait la formation de ce modèle d'apprentissage à la machine. Et on a un bloc également de RegCheck ML, c'est-à-dire comme des blocs ou des briques, des composantes qui permettent de construire et qui peuvent être utilisées ou des fonctionnalités qui peuvent être prises en considération pour connaître les caractéristiques des enregistrements de nom de domaine sur lesquels nous pouvons nous pencher au moment d'essayer de déterminer s'il s'agit d'un nom de domaine qui a été enregistré à des fins malveillantes ou pas.

RegCheck vérifie les enregistrements de noms de domaine et leur attribut une notation de risque entre 1 et 100 points. C'est ce qui va nous indiquer quelle est la probabilité que ce nom de domaine soit utilisé à des fins malveillantes à l'avenir. Un opérateur de registre peut donc utiliser RegCheck et n'a qu'à y saisir quelques informations des sources de cas d'abus ou des étiquettes qui sont utilisées par RegCheck pour permettre à la machine d'apprendre comment identifier ces enregistrements malveillants. On peut voir les nouvelles informations et leur attribuer une notation, un classement. Et à travers des outils de classification, on va essayer d'élaborer une politique pour savoir comment les gérer. Puis, les connaissances de cette application d'apprentissage à la machine permettent de générer cet apprentissage justement en bloc.

RegCheck peut être adapté aux différentes exigences, aux caractéristiques qui sont prises en considération pour évaluer le niveau de risque. Un opérateur de registre va donc devoir connaître les caractéristiques qui doivent être incluses ici. Au moment d'assigner une notation à ce risque et de classer dans un certain seuil un opérateur de registre, il va falloir que l'opérateur de registre sache comment gérer ce niveau de risque, comment atténuer ce risque. Vous allez voir dans les diapos suivantes ce que nous faisons à travers cette application. Je ne sais pas si je peux passer moi-même les diapos. Voilà.

Notre approche à SIDN dans le cadre du .nl est la suivante. Cela fait déjà un moment qu'on utilise un prototype et nous commencerons par le début. Seuls les enregistrements sont dans le fichier de zone, donc on ne fait pas d'enregistrements, même pour les noms de domaine à haut risque. Les noms de domaine récemment enregistrés vont être vérifiés. On commence par un nouvel enregistrement qui est injecté dans l'application, le système de classement va voir cet enregistrement pour essayer de lui attribuer un niveau de risque. Ici, on a un grand filtre où on peut voir quels sont les niveaux de risque, et seuls les opérateurs de registre qui dépassent un certain niveau de risque peuvent accéder à ces informations et passer par un deuxième filtre.

On a ce deuxième filtre où on évalue encore une fois les résultats de RegCheck, c'est une personne qui va le faire. Et si la personne considère qu'il s'agit d'un enregistrement à des fins malveillantes ou qu'il y a quelque chose de bizarre, il va déclencher une réponse sous la forme d'une vérification d'identificateur. On va donc envoyer au titulaire de nom de domaine une demande pour qu'il vérifie son identité. S'il ne le

fait pas dans les trois jours, l'enregistrement est suspendu. Le bénéfice est que nous sommes très diligents dans nos réponses, mais le problème, c'est que cela reste un processus assez manuel. Il nous faut des collègues pour évaluer les résultats et le processus prend pas mal de temps, trois jours.

Et sur, ce Ron, je passe à vous.

RONALD GEENS : Voici ici un exemple du tableau de bord que vous pouvez utiliser, notre interface. Un enregistrement va passer ou échouer cette vérification et grâce à la méthode que nous utilisons pour l'apprentissage à la machine, nous pouvons interpréter ce classement et cette notation pour savoir quelles sont les caractéristiques d'un enregistrement qui ont le plus contribué à cette notation. Par exemple, ici en l'occurrence, c'était le fait que le nom du titulaire de nom de domaine était invalide. On voit que 44 % des demandes de vérification d'identification qui sont lancées par RegCheck commencent à travers une notification automatique du système. On voit que beaucoup du travail de notre équipe de support est déclenché par RegCheck et on voit en même temps que moins de 5 % des titulaires de nom de domaine répondent à ces demandes, ce qui pourrait indiquer que nous sommes effectivement en train d'identifier quels sont les noms de domaine qui pourraient être utilisés à des fins malveillantes.

L'évaluation quantitative ici est difficile, et ce, parce que la seule manière de signer des numéros et de comparer les différents rapports, c'est ce qu'on essaie d'éviter de devoir faire. À mesure qu'on améliorera

RegCheck, il y aura moins de rapports d'utilisation malveillante que nous devrons évaluer. Un exemple d'un fonctionnement correct à 100 % ne montrera pas de rapport et on aura zéro rapport. Si vous voulez savoir quantitativement combien et comment évaluer ces données, je serais ravi d'entendre ce que vous en pensez. Voilà notre approche. En somme, nous essayons de vérifier les enregistrements d'emblée et de voir ce processus de vérification d'identité pour ceux qui sont à haut risque.

Ce projet a commencé en 2020. À l'époque, nous n'étions pas sûrs de pouvoir utiliser l'approche .nl. Donc, nous avons commencé avec le système basé sur les règles, qui est d'ailleurs toujours utilisé. Les règles sont soumises à des évaluations constantes.

Comment ce système fonctionne ? Un titulaire de nom de domaine enregistre son nom de domaine et la combinaison du point de contact et du nom de domaine est utilisée pour évaluer le niveau de risque. Si le risque semble bas, nous incluons le domaine dans le fichier de zone. Si cela n'est pas faisable, nous essayons de vérifier l'identité de façon automatique et ce n'est qu'à ce moment-là que le domaine pourra être placé dans la zone.

C'est actuellement un système basé sur les règles. Nous avons fait une expérience avec le système ML en parallèle, mais ceci est devenu trop complexe. Nous travaillons maintenant ensemble pour commencer à appliquer le système RegCheck. La grande différence, c'est que nous ne faisons pas de délégation si le risque est trop élevé. Et nous utilisons également le ML de façon différente. L'idée est d'avoir la précision la plus élevée possible pour éviter les faux positifs. Nous préférons avoir

quelques faux positifs au lieu d'être 100 % exact. C'est l'un des seuls risques, mais cela nous permet d'être aussi exhaustifs que possible dans la capture des cas d'abus.

Nous avons eu besoin d'une série de données d'entrée pour pouvoir entraîner le système. Et nous prenons également en compte les cas dans lesquels le titulaire de nom de domaine préfère ne pas fournir ces données. Cela nous donne des données supplémentaires et nous espérons que cela nous donne un point de vue plus clair de ce que nous souhaitons freiner, c'est-à-dire en particulier l'hameçonnage. Voilà, c'est tout pour moi. La prochaine, s'il vous plaît.

THIJS VAN DEN HOUT : Pour résumer nos progrès, il y a trois phases de collaboration. Comme Ron l'a dit, nos deux opérateurs de registre ont commencé à faire des expériences avec l'apprentissage automatique pour détecter des enregistrements abusifs. Nous avons créé une étude de faisabilité de RegCheck et nous nous sommes rendu compte qu'il y avait une possibilité de compatibilité entre nos deux registres. À la fin de cette phase d'exploration qui a duré de mars à décembre 2022, nous sommes parvenus à la conclusion que RegCheck constitue une bonne base pour un projet conjoint.

Et en décembre de cette année, nous avons signé un accord de collaboration dans lequel nous avons établi une propriété partagée de la base de code de RegCheck ainsi que de sa propriété intellectuelle. Nous nous sommes engagés à continuer à développer RegCheck et à

migrer notre base code dans une seule et unique version de RegCheck améliorée.

Au cours de l'année qui vient de s'écouler, notre collaboration nous a permis de comprendre que ceci représente toute une série d'avantages au lieu de vouloir produire un système comme cela de façon isolée. Il a plusieurs exemples. Ce serait un peu trop technique de rentrer dans les détails, mais pour la plupart, ce sont des choses qui étaient prises en compte par un registre avant mais pas par l'autre. Maintenant, ces aspects sont pris en compte dans la base de code. Nous avons amélioré nos scores de risque. Nous avons également adopté des aspects géographiques tels que la ville ou le fuseau horaire. Nous avons amélioré la façon dont nous encodons certains champs d'information des titulaires de nom de domaine. Nous avons également modifié la manière dont nous examinons le nom de domaine en tant que facteur de risque en prenant en compte des phénomènes qui ne se passent que dans les cas d'enregistrement malveillant. Et nous avons beaucoup échangé, bien sûr, en matière de conception et de décision de politique afin d'améliorer la qualité de notre code.

Quelques apprentissages pour terminer. Des expériences partagées et des points de vue différents sur l'utilisation malveillante ont une grande valeur, c'est-à-dire voir ce que chacun fait de façon proactive pour lutter contre les abus. Ce partage est extrêmement utile. La collaboration fonctionne, même avec des politiques différentes. Comme vous l'avez vu, les deux approches, celle de .nl et celle de .be, sont très différentes. Mais nous pouvons néanmoins travailler pour le

développement d'une seule application. Il n'est pas nécessaire d'être d'accord sur tout pour pouvoir collaborer.

Nous avons également appris que la collaboration inspire l'innovation du point de vue technique. Nous avons appris de nouveaux aspects techniques les uns des autres, des [inaudible] que nous n'utilisions pas, mais aussi sur le plan politique. Bien sûr, quand il y a plus de personnes qui participent, il y a aussi plus d'opinions. Le travail prend un peu plus de temps, il y a des divergences en matière technique ou en matière de conception ; tout cela n'est pas du tout insurmontable.

Voilà, c'est tout pour nous. Merci.

NICK WENBAN-SMITH : Merci beaucoup. Voilà un exemple de collaboration entre de ccTLD qui travaillent ensemble pour effectivement réduire les cas d'utilisation malveillante. Est-ce que le RegCheck a réduit les cas d'utilisation malveillante ou est-ce qu'il est trop tôt pour le dire ?

THIJS VAN DEN HOUT : Je pense que cela a amélioré effectivement la situation.

NICK WENBAN-SMITH : Très bien, merci beaucoup.

La dernière partie de cette séance consiste plutôt en un dialogue. Nous avons suffisamment de temps pour cela. Je pourrais vous dire que nous avons besoin que tous nos collègues là-bas qui n'ont pas encore pris la parole s'adressent à nous, mais bon. Au final, les grandes conclusions,

c'est que le fait d'avoir réalisé ces projets a réduit les taux d'utilisation malveillante et de manière générale, que ces initiatives sont utiles. Nous allons maintenant vous donner la parole pour des questions. Je vais donner la parole à Joke qui va nous lire une question ou deux sur Zoom.

JOKE BRAEKEN : Première question de John McCormack : « Est-ce qu'il y a un lien pour l'article qui a du parking à environ 20 % dans les TLD ? »

SAMANEH TAJALIZADEHKHOOB : Oui, effectivement, des informations ont été publiées cette année. Je peux vous fournir le lien vers les informations de notre travail.

JOKE BRAEKEN : Une question de Luc Seufer sur Zoom : « Pourquoi est-ce que domaine parking est noté ici ? Est-ce que c'est une forme d'abus ? »

SAMANEH TAJALIZADEHKHOOB : J'ai parlé de domaines parkés dans cette session parce que lorsque nous parlons de domaines qui sont inclus, ce sont tous des domaines actifs ainsi que des domaines qui sont listés sur les listes de réputation et de blocage. Si l'on prend les listes au quotidien pour voir s'ils sont actifs ou pas, vous verrez qu'il y a des catégories dans lesquelles des domaines peuvent être actifs et que par conséquent, ils seraient beaucoup plus nombreux que ceux que nous avons couverts dans notre recherche.

NICK WENBAN-SMITH : Merci.

Y a-t-il d'autres mains levées ?

CHRIS DISSPAIN : Bonjour, Chris Disspain du conseil de la ccNSO.

Peut-être pour Nathan. Je ne vous ai peut-être pas bien entendu, mais vous parlez de l'utilisation malveillante du DNS et ensuite vous parlez de l'Internet en général. Je veux juste comprendre si vous parlez de l'Internet en général ou juste de l'utilisation malveillante.

Ensuite, d'où proviennent vos données ? Et avez-vous une définition fixée de ce que vous considérez comme étant l'utilisation malveillante du DNS pour guider votre utilisation de Compass, etc. ?

NATHAN ALAN : Effectivement, les informations que nous avons utilisées proviennent de URLhaus, OpenPhish, APWG. Nous avons inclus également SpamHaus pour ce projet. Les données disponibles sont sur le site Internet. Je pense que la manière dont nous définissons l'utilisation malveillante est assez semblable aux autres existantes.

NICK WENBAN-SMITH : Une autre question dans la salle. Bart lève la main dans la salle.

ORATEUR NON-IDENTIFIÉ : Merci Andrea. Il y a une question Luc Seufer concernant RegCheck. Il se demandait si les informations complètes sur RegCheck avaient bien été mentionnées.

ORATEUR NON-IDENTIFIÉ : Le pourcentage des faux positifs ? Il a quelque peu fluctué. Cela dépend de ce qu'on appelle un faux positif. Si nous comparons nos résultats aux résultats de Netcraft, nous avons une précision d'environ 20 %. C'est difficile à évaluer parce que RegCheck trouve des choses que Netcraft ne trouve pas et vice versa. Cela peut avoir une influence sur le nombre de faux positifs avéré.

En règle générale, sur le tableau de bord des abus, ce que Netcraft, je crois que 25 % à 50 % font l'objet d'un suivi. Je ne sais pas exactement quels sont les chiffres actuellement.

NICK WENBAN-SMITH : Merci. On a une main levée au fond de la salle.

JUTTA CROLL : Merci de m'avoir cédé la parole. Je suis d'une fondation allemande et à partir de ces présentations et à partir de ce qui a été dit lors de la séance précédente avec le GAC, j'ai bien pu comprendre cette définition de ce qu'est l'utilisation malveillante du DNS qui est spécifique à l'ICANN. Cependant, je me pose une question. Est-ce que le logiciel malveillant est considéré un abus du nom de domaine ? Si ces noms de domaines sont censés divulguer du matériel d'abus ou de pédophilie, est-ce que

c'est un abus d'un nom de domaine ? Est-ce que c'est à en débattre ou cela ne fait pas du tout partie de la portée des discussions à l'ICANN ?

ORATEUR NON-IDENTIFIÉ : Qui veut répondre ?

BRIAN CIMBOLIC : Bonjour Brian, symbolique de PIR. Je voulais apporter une correction. Alan et moi faisons partie du groupe de représentants des opérateurs de registre gTLD RISG.

Mais la question est très bonne. Au moment de parler de l'utilisation malveillante de DNS, en général, on a tendance à ne pas comprendre que quelque chose ne fasse pas partie de ce que l'on définit comme abus du DNS. Cela ne veut pas dire que ce n'est pas terrible et que ce n'est pas quelque chose contre laquelle lutter, mais ici, l'abus tel qu'il est défini correspond à l'abus que l'on peut résoudre au niveau des informations des noms de domaine. Je sais que nous, Nominet, nous avons chacun nos propres programmes pour lutter contre la pédophilie. On s'en occupe, mais le fait qu'on s'en occupe n'en fait pas un cas d'abus du DNS.

Je sais que c'est difficile à comprendre, mais lorsque vous voyez le matériel de pédophilie qu'on rencontre, dans 99 % des cas, on les trouve sur des sites de divulgation de ce type de matériel. Il se pourrait que vous finissiez par voir que les contenus d'un même site Web correspondent toujours à des cas de pédophilie. Pour nous, tout ce que nous pouvons faire est de mettre en suspens tout un nom de domaine.

On empêche peut-être parfois l'abus à des contenus légitimes qui n'ont rien à voir avec la pédophilie.

Mais comme notre outil pour nous occuper est tellement limité, il faut faire très attention à savoir ce que nous pouvons utiliser pour lutter contre la pédophilie. Le fait que ce ne soit pas un abus du DNS ne veut pas dire que ce n'est pas terrible ; cela veut dire que nous ne sommes pas les acteurs qui devraient s'en occuper étant donné les dommages collatéraux que l'on pourrait générer en essayant de s'occuper de ce problème.

JUTTA CROLL : Merci de votre réponse. On a différentes informations des lignes téléphoniques, on voit que le service de partage des fichiers commence à migrer vers les noms de domaine. Je pense que c'est quelque chose qui mériterait votre attention.

ALAN WOODS : C'était juste pour revenir à l'intervention de Chris Disspain. À vrai dire, je pense que Brian a très bien répondu à la question.

Mais pour revenir à ce que disait Chris Disspain, c'était une question à propos des sources. Je ne sais plus très bien comment elle était formulée. Mais je pense qu'à partir de nos expériences avec le groupe de représentants des opérateurs de registre et grâce à nos contacts avec l'ICANN au cours de nombreuses années, nous sommes en mesure de définir quelles sont les sources qui devraient être utilisées. Nous

avons pu convenir que toute source est bonne pourvu qu'elle puisse être démontrée.

Les sources qui apparaissent ici traditionnellement n'ont pas pu être utilisées comme preuves pour pouvoir passer à l'acte et prendre des mesures qu'on attend de nous. Beaucoup du travail qui a été accompli au cours des huit dernières années a littéralement porté sur le fait de faire en sorte que notre débat puisse se pencher sur tout cela. Tant qu'il y a des preuves et que l'on peut prendre des mesures à partir de ces preuves et de ces données, cela devrait être quelque chose que les bureaux d'enregistrement et les opérateurs de registre puissent voir, que l'on prenne des mesures ou que l'on puisse amener d'autres à prendre des mesures.

Si on parle d'outils de mesures des cas d'utilisation malveillante du DNS ou de l'utilisation malveillante en ligne, il faut toujours prendre en considération ce principe clé de la transparence, de la non-« arbitrarité », de nous assurer de donner le crédit aux opérateurs qui cherchent les éléments de preuves, les attentes de transparence et que lorsque des mesures seront prises, on puisse les retracer, comprendre pourquoi cette mesure a été adoptée, quelles sont les preuves sur lesquelles se fonde cette décision. Il faut que l'on puisse garantir qu'on n'a pas ignoré les preuves et les faits. C'est tout. Il faut que ce soit clair. Merci.

NICK WENBAN-SMITH : Merci. Y a-t-il d'autres questions sur le chat ? Parce que j'en ai moi-même. Je veux demander aux membres du panel ce qui suit, parce

qu'on semblerait comprendre comment mesurer l'utilisation malveillante, on a fait des progrès. Je ne sais pas si c'est grâce à la fédération de recherche, si c'est au niveau de Compass, au niveau de l'ICANN. Mais quoi qu'il en soit, chacun définit différemment les gTLD, les ccTLD et leur utilisation malveillante. Or, ici, il n'est pas question exclusivement de politique d'enregistrement ou de taille. Je vois que vous avez chacun vos propres manuels, vos propres procédures. Le .de d'ailleurs qui est le ccTLD allemand est très ouvert. Ils ont une zone très grande qui est incroyablement bien gérée et très sécurisée. Dans un sens, il en est de même dans le cas de .uk ; on a une politique d'enregistrement un peu plus ouverte, comme dans le cas de beaucoup de gTLD. Mais il semblerait que l'on repose sur trois mesures principales.

Les instituts de recherche ne sont pas tous d'accord, mais les tendances sont claires. En général, on a des ordres de magnitude qui ne sont pas toujours les mêmes et c'est ce que je ne comprends pas, parce qu'on n'est pas à quelques chiffres près au niveau des résultats.

Ce serait formidable que vous disiez votre nom pour qu'on puisse comprendre qui est en train de parler.

ROWENA SCHOO : Merci de le signaler.

Vous parliez des différences entre ccTLD et gTLD.

ORATEUR NON-IDENTIFIÉ : Oui, c'était pour voir comment s'entraider.

ROWENA SCHOO : Au moment d'élaborer nos rapports publics et de définir comment ils seraient, on se demandait comment on allait intégrer les gTLD. C'était vraiment un grand défi. Finalement, on les a divisés entre gTLD et ccTLD. Et lorsque je rédige le texte d'explication pour chacun des groupes, j'ai vu qu'il y avait énormément de différence entre les deux groupes. En général, on parle de différences entre les ccTLD, mais c'est vrai qu'entre les gTLD, il y a beaucoup de différences aussi. Certains fonctionnent de manière très fermée, par exemple le .bank et le .pharmacy, c'est-à-dire qu'il y a des restrictions pour ceux qui mesurent et pour les enregistrements. Dans certains des ccTLD, on voit aussi des modules et des modèles très fermés qui ne peuvent pas être appliqués aux sociétés les plus ouvertes. Par exemple, on sait que les collègues norvégiens ont un modèle très restrictif qui réduit ce qui est acceptable.

Mais pour le fait de pouvoir préciser quelles sont les raisons pour lesquelles on a plus ou moins d'abus dans certains cas que dans d'autres, je voulais signaler qu'il y a une étude très intéressante sur laquelle travaille actuellement l'ICANN qui est censée se pencher justement sur ces facteurs-là. Quels sont les différents points de pression ? Quelles sont les différentes problématiques ayant une influence sur l'augmentation des cas d'utilisation malveillante ? Il ne se pourrait qu'il y ait d'autres questions pour lesquelles je n'ai pas de réponse, mais cela vous amènera peut-être à réflexion.

NATHAN ALAN : Dans notre étude, nous avons vu qu'il semblerait qu'il y a plus de contrôles qui ont été adoptés, que ce soit avant l'enregistrement ou après, ou alors pour comprendre les clients. On voit toute une combinaison de facteurs qui permettent de voir cet effet au niveau des occurrences d'abus. Et les opérateurs de registre ont pu commencer à nous tenir au courant de ce qu'ils avaient fait au moment même de l'enregistrement.

NICK WENBAN-SMITH : Samaneh ?

SAMANEH TAJALIZADEHKHOOB : Pour ajouter à ce qui a déjà été dit, comme l'a dit Rowena, je pense que le principal est de pouvoir trouver un facteur pour l'attribuer aux catégories aux fins de la présentation. Mais la règle générale est également que dans l'espace attaque. On peut trouver le facteur le plus représentatif au niveau de la quantité de signalements, et ce n'est en fait que la taille du TLD, rien d'autre.

NICK WENBAN-SMITH : Merci.

Alan.

ALAN WOODS : Ce panel est terrible. Pour la communication, on est très mauvais. Deux commentaires.

Tout d'abord, je ne pense pas que ceci vous aider, mais en tout cas, je voulais dire que récemment, j'ai eu l'expérience d'avoir une attaque très spécifique. Ils faisaient partie d'une campagne qui se concentrait sur un domaine relativement cher. En général, on a tendance à penser que plus le domaine sera bon marché, plus on aura tendance à l'acheter à des fins malveillantes. Mais ici, en général, on avait des points d'entre 30 et 60. Mais le fait est que ces domaines généraient des bénéfices qui auraient pu être en fait une goutte dans la mer.

Les méthodes sont beaucoup plus sophistiquées. Il y a des mesures simples auxquelles on s'attend qui ne sont plus du tout les mêmes. Je sais que plus les débats seront mûrs dans cet espace, plus on verra que les règles ne sont pas suivies. Dans le cadre général de l'ICANN, on a vu beaucoup de cas différents. Je ne sais pas quel était le cas à cette occasion.

NICK WENBAN-SMITH : Ce matin lors de la présentation du GAC, on a vu et on a entendu parler de cette hypothèse qui date d'il y a très longtemps que moins les domaines seront chers, plus ils seront utilisés à des fins malveillantes. Mais ce n'est en fait pas le cas.

On a une main levée.

ROWENA SCHOO : Merci.

Je pense avoir parlé des facteurs géographiques dans ma présentation. La plupart des sources qui sont utilisées ciblent les marques et cela

pourrait ne pas être représentatif en général pour les marques. Dans d'autres pays, on voit des attaques d'hameçonnage qui le signalent un schéma de blocage d'[ISP] et ce sont des attaques qui n'arrivent pas jusqu'au sommet en général. Je pense que la cybercriminalité pourrait également évoluer.

Qu'est-ce qu'on fait à ce moment-là ? Est-ce qu'on essaie de cibler autant de personnes que possible ? Si on utilise un domaine de premier niveau générique qui pourrait être reconnaissable pour le plus grand nombre de personnes, on réussirait plus à le faire. Là on enregistrerait un nom plus cher. Je ne sais pas si on peut tirer des conclusions comme ça, mais cela peut varier d'un rapport à l'autre.

NICK WENBAN-SMITH : Ce que vous essayez de dire est que ce n'est pas que les gens en Allemagne soient plus honnêtes, c'est qu'ils utilisent des noms de domaine génériques de premier niveau parce que le marché est plus grand, si j'ai bien compris.

Bart, vous levez la main ?

BART BOSWINKEL : Oui. Commentaire de John McCormick de Hosterstats. Il rebondit sur une des questions qui a été posée. « On a la question de la confiance. Les ccTLD en général ont plus de confiance que les gTLD dans les marchés généraux mondiaux. En général, on identifie les ccTLD comme si c'était des gTLD, mais la réalité est que les cas d'abus ne sont pas aussi fréquents que dans les gTLD. »

NICK WENBAN-SMITH : Merci pour ce commentaire, John.

Je voulais cependant remettre en cause certaines des questions qui ont été posées et certains des commentaires qui ont été faits.

C'est vrai que les ccTLD sont parfois dans un sens génériques et donc par conséquent des gTLD. Mais si on a des noms de type génériques et qu'on sait tous qu'il existe des ccTLD qui sont également génériques ou quasi-génériques – et je cherche des exemples comme le point .co, .me, .tv. ou .it même puisque les Italiens ont un ccTLD qui semblerait générique. On s'attendrait à ce que ces noms suivent un patron de ccTLD, mais on n'a pas de preuve que ce soit le cas.

ROWENA SCHOO : Merci. C'est très intéressant. L'une des choses que nous commençons à observer par le biais de Compass en ce qui concerne les enregistrements frauduleux ou compromis, c'est que les ccTLD et les TLD génériques ayant été enregistrés par le passé et qui ont été ensuite compromis sont un peu plus visibles dans les ccTLD mais aussi dans les TLD plus génériques. Lorsque l'on voit des nouveaux gTLD qui grandissent plus rapidement, il y a une division des types d'abus. Il y a plus d'utilisation malveillante que de compromission.

NICK WENBAN-SMITH : Si je comprends bien, c'est qu'il n'y a pas tellement plus d'utilisation malveillante dans les ccTLD, c'est plus que c'est un type d'abus différent. Il y a beaucoup de vieux sites Internet qui peuvent faire l'objet

d'une utilisation malveillante. L'utilisation malveillante prend pour cible des sites Internet qui ont des faiblesses plutôt que de s'enregistrer de manière frauduleuse. Je crois que c'est aujourd'hui ce qui apparaît dans la plupart des outils d'évaluation. On pense que l'on compare les gTLD et les ccTLD, mais en réalité, les chiffres ne sont pas très fiables puisqu'il y a beaucoup de nouveaux gTLD. Ceci implique une différence dans ce que l'on compare.

Je pense que nos résultats seraient meilleurs si nous avions un moyen de contacter les titulaires de noms de domaine dont les sites Internet ont été compromis pour qu'il règle ses problèmes de vulnérabilité plutôt que de rendre plus difficile l'enregistrement de nouveaux noms de domaine.

Nous avons beaucoup parlé des listes de réputation et de blocage. Et comme je suis stupide et paresseux, je préfère copier le travail de quelqu'un d'autre. Si je pouvais en acheter un, lequel devrais-je acheter ?

ALAN WOOD : Je pense que c'est un sujet sur lequel nous ne travaillons pas suffisamment dans notre industrie. Nous devons garder à l'esprit le fait que les catégories dans différentes listes de blocage et de réputation soient claires, cohérentes et transparentes.

Je reviens à ce que j'ai dit tout à l'heure. J'utiliserais n'importe quelle liste, tant qu'elle permet de démontrer qu'il y a un abus et que cela nous permet d'agir.

NICK WENBAN-SMITH : Rowena.

ROWENA SCHOO : Merci beaucoup.

Il y a beaucoup de variations dans les taux d'abus et les ccTLD. Nous publions des rapports là-dessus. Les chiffres évoluent. Venez nous voir.

NICK WENBAN-SMITH : Merci beaucoup.

Une question de Bart peut-être.

BRIAN CIMBOLIC : Merci Nick.

Les listes de réputation et de blocage sont un outil important pour permettre des enquêtes plus détaillées. Je vais vous donner des exemples concrets. J'ai eu des cas où il y avait des listes de réputation et de blocage qui m'indiquaient des données pour une intervention alors qu'elles n'étaient jamais incluses auparavant. J'ai même reçu une fois des données, et ce n'est pas tellement que les listes de réputation et de blocage ne fonctionnent pas, c'est plus que c'est un problème avec le DNS.

SAMANEH TAJALIZADEHKHOOB : Pour continuer un peu ce que Brian nous a dit, nous avons fait des études, nous avons utilisé différents indicateurs pour voir ce qui était mesurable dans les listes de blocage en fonction de l'utilisation de l'objectif et voir ce qui était le plus difficile à mesurer. Ce rapport a été présenté cette année lors d'une conférence sur le IDI. Nous pourrons bien sûr vous le fournir.

NICK WENBAN-SMITH : Je suis intéressé par les travaux futurs du comité permanent du DNS. Je pense qu'il faudrait établir une étude là-dessus. Nous sommes en train de considérer une réunion pour travailler un peu plus de manière pratique sur les ccTLD, sur ce qu'ils veulent savoir sur les outils à leur disposition, pour qu'on sache un peu ce qui peut être utile pour ces séances de présentation de ressources et de gestion. Vous pouvez m'envoyer des messages directement, vous pouvez m'aborder dans les couloirs. Si cela vous intéresse, si vous voulez que notre équipe aborde un thème en particulier ou prépare quelque chose en particulier, on est à votre disposition. Il y a toute une question qui est liée au programme d'indicateurs de mesures et aux mesures en général qui pourrait vous intéresser ou pas.

Il ne nous reste plus que cinq minutes. Est-ce qu'il y a des questions dans la salle ? Andrew.

ANDREW BENNETT : je suis Andrew Bennett.

Vous avez dit qu'on avait la possibilité de se présenter pour 22 ccTLD. Je voudrais savoir si on a la possibilité de rentrer ici. Est-ce que l'ICANN va pouvoir persuader davantage de ccTLD à rentrer dans son système ?

NICK WENBAN-SMITH : Peut-être que Samaneh, vous pouvez prendre la parole.

SAMANEH TAJALIZADEHKHOOB : La réponse serait que l'on ne sait pas. On fait tous les efforts possibles pour voir comment fonctionne ce système, quels sont ses bénéfices. Avec le temps, nous avons constaté que certains ccTLD sont parfois préoccupés par la possibilité que leurs fichiers de zone soient partagés ou utilisés. Ceci les inquiète. Donc, on a un rapport qui va être envoyé au contact administratif du ccTLD. La tendance avec le temps et on a constaté cela, c'est que c'est graduel, c'est quelque chose qui va en augmentant. On essaie de demander aux participants de nous envoyer leurs opinions pour que le système puisse être amélioré dans le temps. Ils nous envoient leurs critiques. Pour nous, c'est tout à fait utile.

NICK WENBAN-SMITH : Il y a certains ccTLD qui ont peur que leur fichier de zone soit partagé. Oui, vous avez raison. Puis, le fait d'avoir un tableau de bord, mais ne pas avoir de données sur lesquelles on puisse avoir un impact, il y a des exigences techniques ici pour établir cela.

Je vois qu'il y a quelques commentaires dans le chat.

BART BOWSINKE : Il y a plusieurs commentaires. Le premier et c'est une question au panel : « Est-ce que les enregistrements pour ces domaines de gTLD sont inférieurs aux enregistrements des domaines de ccTLD ? Est-ce que l'on tient compte du fait que certains logiciels vont permettre de modifier ces chiffres ? »

Puis, nous avons un commentaire de Alexander Hugla : « Les listes de réputation privées sont fondées par des compagnies privées. On ne peut pas leur faire confiance parce que ce sont des questions de clientèle. »

NICK WENBAN-SMITH : J'ai vu quelques listes de réputation, des listes de blocage qui ne sont pas toujours de qualité. Par conséquent, la décision de bloquer est compliquée à prendre. Je le comprends bien, on ne peut pas toujours faire confiance à ces listes.

Nous avons présenté notre travail. Nous n'avons pas encore complètement terminé ce travail. Au cours des dernières réunions de l'ICANN, nous avons commencé à présenter les données. À Cancún quelqu'un nous a suggéré même de faire davantage de recherches et de continuer les discussions sur ces thèmes.

Pour la réunion de l'ICANN77, il y a eu des suggestions. On a essayé de répondre à ce qui a été dit. On essaie de proposer à la communauté ce que la communauté nous a demandé de faire, d'élaborer des travaux dans ce sens. C'était quatre suggestions auxquelles nous avons répondu.

Notre objectif maintenant est de continuer à travailler sur d'autres questions qui nous ont été posées, aussi d'autres travaux qui nous ont été demandés. C'est une liste qui n'est pas établie. Nous voulons répondre aux demandes qui nous sont faites. Si certains thèmes vous intéressent, dites-le-nous. Si certains thèmes cessent de vous intéresser, bien sûr dites-le-nous aussi. Vous pouvez nous contacter. Personnellement, je trouve que les exemples sont très utiles. Partager les données en fonction des registres des ccTLD ou des gTLD, avoir des données de des différents TLD, c'est très utile pour nous. Ceci nous permet d'avoir de bons exemples sur la façon dont on peut mieux travailler avec les bureaux d'enregistrement. Il y a certains bureaux d'enregistrement qui sont dans la salle, ce qui est fantastique, mais nous devons travailler de manière collective. Il faut que ce soit vraiment une collaboration entre nous. Ce sera un des principaux thèmes de travail lors de notre prochaine réunion de Porto Rico.

Nous sommes en retard, mais nous allons prendre un dernier commentaire.

ROWENA SCHOO : Personnellement, je suis très intéressée par tout ce qui concerne les plans d'encouragement, voir si les opérateurs de registre peuvent travailler avec leur clientèle, est-ce que les TLD metten en place ce type de plan d'encouragement pour obtenir ce type de données et autres.

NICK WENBAN-SMITH : C'est une très bonne suggestion.

Nous allons terminer ici notre séance. Merci d’avoir contribué tous. Je remercie les personnes qui ont participé à ce panel. Cette réunion est maintenant terminée.

[FIN DE LA TRANSCRIPTION]