FR

ICANN84 | Réunion générale annuelle – DNS Women
Mercredi 29 octobre 2025 – 16h30 à 17h30 IST

MICHELLE DESMYTER

Bonjour et bienvenue à toutes et à tous à cette séance « Les femmes du DNS ». Je m'appelle Michelle Desmyter, je serai la responsable de la participation à distance pour cette séance.

Veuillez noter que cette séance est enregistrée et régie par les normes de comportement attendu de l'ICANN, ainsi que la politique anti-harcèlement de la communauté de l'ICANN. Lors de cette séance, les questions et les commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre questions-réponses sur Zoom.

L'interprétation lors de cette séance sera assurée en français, anglais et espagnol. Si vous souhaitez vous exprimer lors de cette séance, veuillez lever la main dans Zoom. Lorsqu'on appellera leur nom, les participants à distance pourront activer leur micro sur Zoom, et les participants en présentiel utiliseront un micro physique. Veuillez donner votre nom pour l'enregistrement ainsi que la langue dans laquelle vous allez parler si vous parlez une autre langue que l'anglais, et veuillez parler à un rythme raisonnable.

Sur ce, je vais donner la parole à Vanda Scartezini.

VANDA SCARTEZINI

Merci beaucoup à toutes et à tous, vous qui êtes venus participer à cette séance aujourd'hui. En général, il y a beaucoup de conflits horaires dans les agendas de chacun, chacune, lors des réunions de l'ICANN, mais j'apprécie vraiment l'effort que vous faites afin de participer à cette séance avec nous cet après-midi.

En général, nous donnons la parole en premier à notre éminent orateur, ou éminente oratrice, invité. Très souvent ce sont des membres honoraires ou des membres du conseil d'administration un membre honoraire qui est tout le temps avec nous, c'est Maarten Botterman. Maarten Botterman, je vais vous céder la parole.

MAARTEN BOTTERMAN

Vous auriez pu me prévenir que j'allais devoir prendre la parole. Merci beaucoup de m'avoir accueilli ici aujourd'hui. Je viens de voir qu'il y a un autre membre honoraire qui vient de rentrer dans la salle. C'est toujours un plaisir de voir l'ICANN évoluer, et ce depuis les neuf ans que je fais partie du conseil d'administration.

Ce réseau, ici aujourd'hui, a aussi émergé au fil du temps, et cela représente une véritable valeur ajoutée. Cela vous permet de vous aider les uns les autres, et de reconnaître la valeur de ce que vous faites ensemble. C'est incroyable. Donc je pense surtout vous remercier, et remercier celles et ceux qui ont fait de ceci une réalité. Et j'apprécie toujours le fait d'être invité à vos séances,

mais je voudrais surtout vous remercier et vous applaudir. Et j'apprécie aussi beaucoup le fait que maintenant votre groupe a une portée mondiale. Félicitations.

VANDA SCARTEZINI Merci beaucoup. Maintenant je peux donner la parole à l'autre de nos membres honoraires. Notre ancien président du CA, Steeve Crocker. Je vous en prie, vous avez la parole Steve.

STEVE CROCKER Merci beaucoup Vanda. C'est toujours un honneur pour moi d'être ici et j'ai été très honoré quand on m'a rendu membre honoraire de ce groupe. Il y a différentes choses qui me viennent en tête, certaines qui sont peut-être un peu plus amusantes que d'autres. J'accorde vraiment beaucoup de valeur à ce groupe, et je pense qu'il est très important. Moi, ma maison, on va dire, au sein de l'ICANN c'est le SSAC. Bon, pardonnez-moi, je dévie un peu.

Il y a une autre réunion du SSAC qui a lieu en même temps que celle-ci, et en fait je me suis rendu compte que j'avais envie de venir à cette réunion aussi. Donc j'accorde toujours la préférence à votre groupe. Bon j'avais des blagues en tête à faire. Je veux dire comment on rencontre les femmes à l'ICANN ? Et bah voilà, c'est ici, à cette réunion.

La structure des unités constitutives à l'ICANN a certaine spécificité, notamment par rapport là où définit les limites. Et je pense qu'ici nous sommes dans l'une des plus importantes unités

constitutives, même si elle n'a pas vraiment un groupe de représentants spécifique. Mais je pense que ça représente votre importance.

VANDA SCARTEZINI Merci encore, et merci d'être ici avec nous aujourd'hui. J'espère que vous continuerez à assister à nos réunions pendant de nombreuses années. Je voudrais maintenant donner la parole aux autres membres du CA. Je vois Catherine là-bas. Catherine, je vous en prie, rapprochez-vous du micro et faites-nous part de vos mots de bienvenue à notre communauté.

CATHERINE Merci beaucoup. J'étais justement en train de dire « mais il y a énormément de membres du CA ici aujourd'hui », donc je ne vais pas trop m'attarder. Je voudrais juste dire que c'est un plaisir pour moi d'être ici, et je ne vais pas revenir sur votre blague, de comment rencontrer des femmes à l'ICANN. Mais c'est toujours un plaisir pour nous de participer à ces réunions-ci.

VANDA SCARTEZINI Merci Catherine. Léon, à votre tour.

LÉON SANCHEZ

Merci beaucoup Vanda, et merci beaucoup à toutes et à tous de nous accueillir. C'est un plaisir et un véritable honneur de vous retrouver comme c'est le cas à chaque réunion de l'ICANN. Tout ce que j'ai à dire, et bien c'est continuez à faire le magnifique travail que vous faites. Continuez de sensibiliser les gens aux questions d'égalité de genre au sein de notre organisation. Merci Vanda, merci à toutes les femmes ici présentes, au sein de ce groupe des femmes du DNS.

VANDA SCARTEZINI

Merci Léon. Moi, j'attendais le moment en fait où on allait revenir au sein de région pour vous accorder le titre de membre honoraire de notre groupe, mais en fait, au final, on ne retourne jamais dans nos régions. Je pense qu'on devrait revenir à ces réunions, mais bon. Quoiqu'il arrive, vous serez toujours là où que l'on soit. Merci beaucoup pour vos mots chaleureux, et commençons donc maintenant. Ah, je vois Miriam. Miriam, à vous.

MIRIAM SAPIRO

Oui, pardonnez-moi, j'avais quelques minutes de retard. C'est un plaisir d'être ici, et de voir autant de visages familiers dans la foule, et aussi de voir des visages que je ne connais pas encore et que j'ai hâte de rencontrer. J'en suis à ma deuxième année au CA. J'ai été désignée par le comité de désignation et ça a été un véritable honneur. D'une certaine façon, c'est vous qui m'avez nominée. Et comme Catherine l'a dit, c'est une collègue incroyable, et je ne voudrais pas prendre trop de temps sur cette réunion, mais je

voudrais vous redire ce que Vanda m'a dit en privé, c'est-à-dire que vous êtes vraiment un outil puissant, un groupe de femmes puissant. Et nous vous sommes reconnaissants. Nous avons beaucoup de béatitude pour ce que vous avez fait et pour ce que vous faites au jour le jour. Aussi, continuons sur cette lancée. Montrons l'exemple aux générations à venir. Essayons de tenter d'inspirer la nouvelle génération de dirigeant. Merci.

VANDA SCARTEZINI

Merci beaucoup Miriam. Merci, Miriam, pour votre présence ici aujourd'hui. Je voudrais vous rappeler que Becky n'est pas ici avec nous aujourd'hui, mais elle est très active, très impliquée à chaque réunion. Parfois c'est impossible pour elle de nous rejoindre, parce qu'elle a des conflits horaires, mais voilà. Je voudrais remercier Becky aussi, ici aujourd'hui, parce qu'elle est très souvent avec nous et qu'elle nous a toujours soutenus dès le début. Et bien sûr, j'apprécie la présence de tout le monde à cette réunion.

Alors nous allons peut-être changer un petit peu notre ordre du jour parce que notre membre fondatrice Cheryl a un conflit horaire. Elle prend des photos, figurez-vous, dans une autre salle. Aussi, peut-être qu'on ne va pas pouvoir commencer par l'entendre elle en premier. Il y a 10 ans, jour pour jour, nous étions ici à Dublin, et ce n'était pas la première fois, mais regardez cette photo avec le pont. On avait eu un temps très très beau. Bon, il n'y avait pas eu autant de pluie, il ne faisait pas si froid, il n'y avait pas autant de vent que cette fois-ci, mais on a eu un petit déjeuner qui

avait été sponsorisé, parrainé, par Amazon. C'est à ce moment-là qu'ils ont commencé à nous soutenir. Et voilà, vous voyez les personnes qui étaient là au début, sur cette photo. Certaines de ces personnes ne sont plus avec nous, d'autres personnes sont encore avec nous. Mais Cheryl reviendra après avoir pris les photos dans cette autre salle, et elle viendra nous rejoindre et elle vous parlera, justement, de ce temps qui s'est écoulé, et elle nous parlera de tout cela. Ah, la voilà ! Mais votre timing est parfait. Vous êtes là, pile-poil, au bon moment.

CHERYL LANGDON-ORR Mais j'attendais dehors, figure-vous.

VANDA SCARTEZINI Et bien, je voudrais vous remercier et je voudrais qu'on l'applaudisse. Bien, prenez votre temps, et prenez place et puis ensuite on vous donnera la parole. Donc au final, on ne va pas changer l'ordre des oratrices à notre ordre du jour.

CHERYL LANGDON-ORR Bonjour Mesdames et quelques messieurs. Je m'appelle Chery Langdon-Orr. Je suis l'une des fondatrices de ce groupe, et au départ on était autour d'une table. Je pense qu'on était sept, et on a pris un petit déjeuner. Voyez combien on est maintenant. Je pense qu'on peut dire qu'au cours des 10 dernières années qui se sont écoulées depuis notre première fois à Dublin, rappelez-vous, notre groupe a été formé en 2009, donc on est maintenant bien

plus âgés. Pardonnez-moi, je reprends mon souffle. Je présente mes excuses aux interprètes qui m'interprètent.

Bon, quand on se penche sur cette photo, on se rend compte qu'il y a beaucoup de femmes présentes, mais quand on prend des photos aujourd'hui, c'est un groupe bien plus grand. Bon je voudrais qu'on prenne un peu de temps pour réfléchir. Il y a beaucoup de ces femmes, sur cette photo, qui ont depuis occupé des fonctions à très hautes responsabilités dans le monde de la gouvernance de l'internet, dans tout ce qui concerne l'adressage, le nommage, la gestion des numéros. Et certaines de ces dames, à cette époque, étaient de nouvelles recrues, avaient une expérience dans le domaine technologique et se demandaient quoi faire dans notre espace. Et au fil de ces 10 dernières années, ces « diplomées », si on peut les appeler comme ça, et je pense que vous serez d'accord avec moi, se sont rendues compte que tout est une question de confiance et de confort. C'est-à-dire qu'il s'agit de savoir qu'on n'est pas seules, et qu'il y a toute une série de femmes qui peuvent vous inspirer, et espérons qu'à votre tour vous inspirerez d'autres femmes de façon à ce qu'on soit toujours présentes.

Je suis immensément fière du fait que des femmes disent que j'aimerais faire cela avec des femmes au niveau local. Et maintenant, nous avons vu essaimer un nombre de chapitres locaux, de femmes du DNS. Je tenais à vous le dire cela devrait vous intéresser, que vous soyez dans un État insulaire, ou dans un très grand pays, c'est toujours possible à faire. Je sais que, quelque

part dans cette salle, il y a quelqu'un qui a dit « moi j'ai déjà parlé à plusieurs personnes et nous envisageons de lancer un nouveau chapitre » et j'ai dit non c'est pas à moi qu'il faut s'adresser, mais à Vanda. Donc il y a, en tout cas une personne, que cela intéresse.

Sur ce, je voudrais que vous preniez quelques instants pour réfléchir, même pas en regardant cette photo, mais donc vous vous souvenez les 500 et quelques entre nous. Nous avions donc ce réseau qui nous permet de développer notre confiance, de partager nos réussites et de faire en sorte que le cheminement des femmes dans cette catégorie, donc de l'information et de la communication, soit donc visible pour tous.

Merci beaucoup, je n'ai rien d'autre à ajouter.

VANDA SCARTEZINI Voilà, où que vous soyez, sachez qu'il y a des femmes qui ont besoin de soutien, qui souhaitent être réunies, se réunir et faire partie de notre groupe, partager leurs expériences, leurs témoignages, et même faire des affaires. Nous avons fait des affaires.

Il est intéressant de faire partie de cette communauté qui existe dans le monde entier. Donc si vous êtes chez vous, à votre table, comment auriez-vous la possibilité de rencontrer des personnes qui ont les mêmes buts, les mêmes intentions, de rendre l'internet plus ouvert, plus inclusif, et beaucoup plus intéressant pour les générations futures. Nous souhaitons la bienvenue aux plus

jeunes. Nous sommes sur le point de départ. Notre temps est limité, mais bon, nous restons quand même. Donc elle est très têtue peut-être.

Alors j'apprécie le contact. Moi je suis quelqu'un qui aime répondre à tous les mails. Je vais donc répondre à tous les messages sur WhatsApp, LinkedIn, etc. pour rester en contact. Restez en contact avec nous. Et donc renforçons notre implantation dans le monde, et créons des opportunités dans vos pays, vos régions. Créons ces possibilités pour les femmes.

Merci beaucoup, et maintenant, nous allons entendre une panéliste très intéressante. Alors nous allons écouter des idées sur ce que nous faisons dans le monde par rapport à l'utilisation malveillante du DNS. Nous allons partager des expériences, des idées sur la façon de traiter ce sujet, qui est complexe. C'est une situation complexe. J'ai demandé à Hadia, Margarita, Samaneh, c'est bien comme ça qu'on prononce votre prénom, Samaneh ? Et moi-même aussi, car il y a au Brésil des expériences qui peuvent servir à d'autres pays en développement. Donc je pense que nous pouvons apporter des contributions aux autres pays concernant les problèmes auxquels tout le monde est confronté, relatifs à l'utilisation malveillante du DNS. Et nous allons donner la parole, tout d'abord, à Hadia, qui est notre présente du chapitre égyptien. Merci Hadia.

HADIA ELMINIAWI

Merci beaucoup Vanda. Alors je vais prendre quelques instants pour vous remercier et remercier donc Cheryl aussi, les fondatrices des femmes du DNS. Et la raison pour laquelle j'ai accepté ce rôle de dirigeante au sein de l'ICANN, c'est en raison des femmes du DNS. C'était lors d'une réception, et c'était ma deuxième réunion de l'ICANN. Et donc à ce cocktail des femmes du DNS, vous parliez des rôles de direction au sein de l'ICANN et vous nous encouragiez à postuler. J'ai pris la brochure que vous distribuiez et je suis allé sur le site. J'ai posé ma candidature au NomCom, et c'est ainsi que j'ai été lancée. C'est une histoire vraie. Et maintenant, je vais commencer cette présentation que j'ai à vous livrer.

Donc le DNS c'est l'épine dorsale du DNS. Il traduit les noms de domaines en adresses IP et cela nous permet d'atteindre des sites web et des services facilement. Mais, donc en raison de son rôle central, le DNS est aussi une cible fréquente pour les personnes malveillantes, les acteurs malveillants. Donc nous allons examiner de plus près la façon dont le DNS est exploité. Il y a des rapports qui ont identifié les formes les plus courantes d'utilisations malveillantes du DNS. Et nous allons voir comment la communauté At-Large peut jouer un rôle important en sensibilisant, en promouvant les meilleures pratiques et en déployant des efforts, pour rendre le DNS plus sécurisé et plus stable pour tout le monde.

L'utilisation malveillante du DNS peut être un usage des infrastructures de DNS de façon sapes la stabilité, la sécurité et la confiance de l'internet. Donc cette utilisation malveillante c'est

une action délibérée. Quelqu'un qui utilise l'infrastructure du DNS ou des noms de domaines pour se livrer à des activités préjudiciables, par exemple créer un compte en banque frauduleux, ou créer des domaines qui diffusent des virus, ou des logiciels malveillants. Et donc il peut s'agir d'un domaine qui est piraté, ou infecté, par un logiciel malveillant, sans que le détenteur soit au courant, ou par exemple des collisions de noms, lorsqu'il y a un chevauchement avec un nom de domaine public. Et parfois il y a un préjudice non intentionnel, cela peut arriver aussi. Donc l'ICANN tient compte des usages malveillants suivants, les réseaux zombies, les logiciels malveillants, le dévoiement et le hameçonnage, et les courriers indésirables. Diapositive suivante.

Je vais passer en revue très rapidement les éléments suivants. Les réseaux zombies sont un groupe d'appareils qui ont compromis des appareils. Ce sont des réseaux qui ont porté préjudice à des appareils. Donc les réseaux zombies inondent des services ou des appareils avec des trafics et causent des perturbations. Les réseaux zombies sont des outils fréquemment utilisés dans l'usage malveillant du DNS et dans les cyberattaques, car ils permettent des attaques à grande échelle. Diapositive suivante s'il vous plaît.

Le hameçonnage. Ici, l'utilisateur est incité à cliquer sur un lien malveillant où il y a donc des usurpations de noms de sites web malveillants sont utilisés. Donc le domaine est piraté ou malveillant. Les utilisateurs doivent bien vérifier les URL, ils doivent donc utiliser les utilisations multifactorielles et nous

parlerons du rôle de l'At-Large en ce sens. Diapositive suivante s'il vous plaît.

Les logiciels malveillants. Là, il n'est pas nécessaire de cliquer quoi que ce soit. Il suffit d'ouvrir un site malveillant, et un code malveillant peut être installé dans votre appareil, et il sera en veilleuse et votre appareil est compromis. Alors que faire dans ce cas ? Il est très important de faire que notre navigateur, nos applications, notre système d'application aient toutes les protections à jours. Et la communauté At-Large peut avoir un rôle à jouer. Diapositive suivante s'il vous plaît.

Donc maintenant le dévoiement, c'est une forme d'usage malveillant du DNS comme le hameçonnage. La différence ici, c'est que l'usage malveillant se situe au niveau du DNS. Et pour cela, il y a les DNSSEC, donc la mise en œuvre des DNSSEC peut donc vous protéger contre l'utilisation malveillante du DNS. Diapositive suivante.

Maintenant ce sont les courriers indésirables. Ici ce sont les courriers de masses, donc des messages qui sont envoyés de façon non autorisée en grande quantité. Diapositive suivante s'il vous plaît.

À gauche, nous avons un tableau. C'est le rapport Interpole qui montre le hameçonnage qui est l'attaque la plus suivante. Le rapport d'évaluation de fraude financière mondiale de 2023-2024 nous dit que le hameçonnage ciblé et donc la pratique la plus courante, donc l'usurpation d'identité, les fraudes financières à

travers le monde sont effectuées de cette façon. Le rapport d'évaluation de 2025, d'évaluation des menaces en Afrique par Interpole, classe les différents types d'activités en fonction des données obtenues par les forces de l'ordre. Le hameçonnage c'est le cybercrime le plus répandu.

Alors At-Large, que peut-il faire ? La communauté peut jouer un rôle clé dans le combat de l'utilisation malveillante du DNS, en faisant des campagnes de sensibilisation, le développement des connaissances, l'éducation, la coopération et les sondages. Hier, nous avons convenu de créer un groupe de recherche. Et donc la communauté At-Large, la communauté des parties prenantes mondiales, nous pouvons ensemble promouvoir les meilleures pratiques, mener des sondages et donc demander à ce que les meilleures pratiques soient utilisées. Diapo suivante et ce sera la dernière.

Cette diapo porte sur l'AFRALO et les efforts de sensibilisation et notre plan de sensibilisation. AFRALO continue à travailler à une stratégie non sans noter toutes les RALO. Tout le monde a un plan similaire de communication et de sensibilisation. Donc nous continuons à travailler à ces initiatives pour avoir une communauté informée quant aux utilisations malveillantes du DNS. Et les résultats de nos efforts consistent notamment à promouvoir les compétences technologiques, concernant la mise en œuvre du DNSSEC, par exemple, et nous organisons aussi des programmes de mentorat, et de renforcement de capacités grâce à des webinaires. Nous menons des campagnes afin d'informer les

utilisateurs finaux concernant les différentes formes d'utilisations malveillantes du DNS, telles que le hameçonnage. Et nous leur apprenons comment utiliser le filtrage, l'authentification à multifacteurs, etc., et nous les informons aussi de l'importance de mettre à jour ces navigateurs pour se protéger de logiciel malveillant. Nous coopérons aussi avec avec la GSE de l'Afrique pour améliorer l'adoption de la DNSSEC. Nous travaillons aussi au niveau de la coopération internationale, qui est très importante. Les membres de l'AFRALO peuvent aussi faire part de leur réussite au travers de webinaires spécifiquement dédiés à cela, ou au travers de nos réunions mensuelles ou de notre newsletter. Hier, nous avons parlé du groupe de réflexion, et l'AFRALO dispose déjà de déclarations concernant l'utilisation malveillante. Peut-être qu'on pourrait commencer par passer en revue ces déclarations, se repencher sur ces déclarations, et se demander ce qui a été mis en œuvre, ce qui doit encore être fait. Ça pourrait être un bon début. Et sur ce, je voudrais vous remercier, et je cède la parole à Vanda. Merci.

VANDA SCARTEZINI Merci beaucoup Hadia, pour cette présentation très intéressante. Je pense que les RALO, effectivement, doivent aller plus loin encore et interagir davantage entre elles, car ces logiciels malveillants, toutes ces utilisations malveillantes du DNS, ne viennent pas forcément de vos pays. Très souvent, il y a une circulation à travers les différents pays pour rendre la détection plus difficile. Donc je pense que nous aurions besoin d'un accord

entre les RALO afin de nous aider à suivre tout cela de manière plus efficace. Merci.

Alors la prochaine oratrice. Margarita, vous avez la parole.

MARGARITA VALDES

Merci beaucoup, Vanda. Merci de m'avoir invitée. Je m'appelle Margarita Valdes, je viens de l'opérateur de registre .cl, qui est en charge des TLD au Chili. Nous appartenons à l'université du Chili, qui est la plus grande université publique du pays. Je voudrais remercier Hadia d'avoir expliqué les questions très techniques, parce que je vais passer cette partie de ma présentation. Diapo suivante.

Donc voilà le DNS, vous savez ce que c'est. Au début on avait des numéros, et puis ensuite on devait se rappeler des adresses des noms. C'est pourquoi on a établi les noms de domaine. Merci à John Postel d'avoir établi ce système. En bref, le DNS, souvent on dit que c'est un arbre inversé. C'est-à-dire qu'on a les racines en surface, et les branches, les ramifications, qui sont le système de noms de domaine divisé en gTLD et ccTLD. Pourquoi cette différence ? Et bien tout simplement parce que les codes pays sont des codes à deux lettres, tandis que pour tout le reste, c'est trois lettres ou plus. Diapo suivante, s'il vous plaît.

Bon je l'ai dit, les plus grands acteurs de ce système du DNS ce sont notamment les gTLD et les ccTLD. Alors, quand est-il des utilisations malveillantes techniques du DNS ? Hadia l'a mieux

expliqué que je pourrais le faire. Et bien ce sont des utilisations du DNS visant à escroquer les personnes, à tromper les personnes. Donc il s'agit de comportement malveillant pour se servir du DNS à des fins de fraudes.

S'agissant du Chili, je vais vous faire part de notre expérience. Avant de 2020, nous avions une réglementation permettant la validation des enregistrements conformément à l'article 17 de nos contrats de services pour l'enregistrement. On l'appelle « reglamentación » en espagnol, et les temps d'enregistrements étaient très longs et notre temps de réaction était très limité. En 2020, nous avons apporté une modification à nos réglementations afin qu'elles incluent un nouvel article, l'article 6D concernant la désactivation de noms de domaines dans les cas d'utilisation malveillante technique du DNS comme mesure de prévention. À l'heure actuelle, nous avons la possibilité de suspendre. Donc une désactivation, ce n'est pas radié un nom de domaine, c'est plutôt de le suspendre, de suspendre le service de ce nom de domaine de façon à ce qu'on puisse analyser dans un temps très bref quelles sont les activités liées à ce nom de domaine et la façon dont on peut prévenir toute utilisation malveillante de ce nom de domaine.

Quel est le protocole actuel ? Pour le moment, nous pouvons suspendre l'opération d'un nom de domaine lorsqu'il a été vérifié que ce nom de domaine a été enregistré notamment pour des

raisons d'hameçonnages, pour mettre en œuvre des réseaux zombies ou des logiciels malveillants.

Alors vous voyez sur cette diapositive les différentes étapes de notre travail. Nous sommes disponibles pour recevoir tout type de rapport de dénonciation, à cette adresse que vous voyez à l'écran abuse@nic.cl, ensuite nous menons une analyse technique qui permet d'évaluer de manière détaillée le cas de ce nom de domaine suspicieux. Ensuite, nous pouvons classer ce nom de domaine comme compromis ou malveillant, parce que parfois les rapports que l'on reçoit concernent un site qui est compromis dans le sens où ce n'est pas un nom de domaine qui a été enregistré afin d'être utilisé à des fins malveillantes. Parfois c'est juste qu'il a un problème de sécurité lié à ce site web, ou lié au serveur qu'utilise le titulaire de nom. Donc ce n'est pas le nom de domaine en soi qui pose problème. On a donc introduit cette différence entre « compromis » et « malveillant ».

Ensuite, on peut décider d'entreprendre des actions, par exemple envoyer une notification ou carrément désactiver le nom de domaine, si nous sommes quasiment certains qu'il s'agit en effet d'un nom de domaine enregistré à des fins malveillantes. Alors dans le premier exemple. Nous avons un site compromis, piraté. Le nom de domaine légitime a fait l'objet d'une atteinte. Le propriétaire de ce nom de domaine reçoit une notification directement concernant ce problème de sécurité. Et dans le deuxième exemple, on a un enregistrement malveillant, c'est-à-dire que le nom de domaine a été créé à des fins malveillantes. À

ce moment-là, ce nom de domaine est automatiquement désactivé conformément à notre protocole établi.

Alors quand est-il des critères de suspensions. Comme je l'ai dit, nous avons un nouvel article, l'article 6 D. L'évaluation que nous menons porte sur la création de ce nom de domaine afin de savoir s'il a été créé à des fins malveillantes. Nous nous penchons sur le moment de l'enregistrement, les domaines similaires associés, les informations de contact, les comportements que l'on peut observer et la désactivation requière une réponse unanime des personnes qui mènent l'évaluation. Il s'agit d'une équipe de 11 experts.

Sur ce graphique, vous pouvez voir le nombre total de rapports de dénonciation entre guillemets que nous avons eu, et il y a ici le détail du nombre réel de cas d'utilisation malveillante du DNS. Il y a deux autres chiffres à l'écran, donc les cas qui relèvent de l'article 17, c'est-à-dire que là on peut agir avant de désactiver le nom de domaine. On peut donc demander au titulaire du nom de domaine de nous donner des informations fiables selon lequel il s'agit d'un véritable titulaire de nom qui est sérieux. Une fois qu'ils reçoivent cette information, les titulaires de noms ont cinq jours pour répondre à notre courriel et nous dire voilà, telle est mon adresse, je suis une véritable personne, ou alors je suis personne morale, une entité juridique. De cette façon, nous pouvons vérifier cette information et donc retirer ce cas-là de nos cas d'utilisation

malveillante du DNS. Et puis on a les cas qui relèvent de l'article 6, il y en a 92.

Quels sont nos plans pour l'avenir ? Et bien nous allons tenter d'automatiser de manière progressive ce processus. Nous allons tenter d'utiliser l'IA afin d'être plus proactifs et de pouvoir réagir plus rapidement, car ici la vitesse est essentielle lorsqu'on remarque d'utilisation malveillante du DNS. Nous voulons avoir un système de ticketing, un système de gestion centralisé pour suivre de manière efficace les cas qui font l'objet d'une notification afin d'améliorer la traçabilité des incidents. Nous voulons établir un panel de contrôle qui va se spécialiser dans le suivi en temps réel des utilisations malveillantes du DNS. Et nous voulons aussi mettre en place des révisions continues, et donc mettre à jour de manière permanente les protocoles d'actions basées sur les menaces, les meilleures pratiques internationales et les retours opérationnels que nous recevons.

Et bien sûr, nous sommes très engagés s'agissant de la sécurité numérique. Nous sommes bien conscients du fait que nous sommes un acteur clé au sein de l'écosystème numérique du Chili. Donc nous travaillons en étroite coopération avec d'autres entités qui sont impliquées dans la sécurité numérique du Chili, de façon à atténuer les utilisations malveillantes du DNS. Notre mission est de garantir que l'espace de nom .cl soit un environnement sûr que peuvent utiliser les utilisateurs finaux au sein de l'écosystème numérique du Chili.

Alors le protocole d'évaluation unanime garanti par 11 experts nous permet de garantir que chaque décision prise quant à la désactivation d'un nom de domaine soit raisonnable, juste, et qu'elle permet un équilibre entre sécurité et respect des droits des titulaires de noms de domaines légitimes.

Alors nous avons différents canaux de communication. Cette présentation a été établie grâce à mon travail et celui de Guillermo Lama, notre CISO. Nous avons adresse e-mail : abuse@nic.cl et vous voyez également nos propres adresses mail personnelles : mvaldes@nic.cl et également glama@nic.cl. Merci beaucoup.

VANDA SCARTEZINI Merci beaucoup. Nous savons toujours effectivement que les ccTLD ont plus de capacité à mieux gérer le système. Et ils peuvent le faire s'ils le veulent, surtout s'ils veulent faire en sorte que les processus soient plus efficaces pour les communautés dont ils servent les intérêts.

MARGARITA VALDES Oui, et d'ailleurs je voudrais ajouter le fait qu'au sein de la ccNSO nous avons le comité permanent sur l'utilisation malveillante du DNS, le DASC, car au sein de la ccNSO nous nous voulons vraiment aider toutes celles et ceux qui veulent essayer de prévenir les utilisations malveillantes du DNS.

VANDA SCARTEZINI Avant de donner la parole à Samaneh, Maarten souhaiterait poser une question.

MAARTEN BOTTERMAN Merci pour cette présentation, merci Margarita, merci de faire tout cela. On voit que vraiment quelque chose a été atteint au vu de cette courbe. Maintenant il y a donc ces études de cas, et il y a ces 11 prestataires de services. Est-ce qu'il est possible de tout réunir et de créer un document des meilleures pratiques, car les informations qui seraient retirées seraient très précieuses ?

MARGARITA VALDES Oui, la réponse est oui. C'est un travail très intéressant que nous faisons au Chili. Les panélistes sont des experts, ils proviennent des sections les plus anciennes de notre organisation. Il y a des ingénieurs, des avocats, des clients, des responsables du service à la clientèle, et donc tous les participants à ce système d'opérateurs de registre. Donc ils ont des compétences qui sont diverses et variées, qui vont au-delà des compétences techniques, ce qui est très important pour ce type d'enregistrement. Merci.

VANDA SCARTEZINI Merci. Et donc Samaneh, vous avez la parole. Est-ce qu'il ya encore une question qui peut-être posé ? Nous avons un autre intervenant. Je ne vous avais pas donné la parole, mais maintenant nous vous donnons l'occasion de dire bonjour et de nous permettre de vous saluer.

RAUL ECHEBERRIA

Merci, je vous félicite pour cette réunion. C'est un plaisir d'être parmi des femmes aussi impressionnantes, aussi inspirantes. Merci Margarita. Je m'appelle Raul Echeberria, et je vais donc commencer mes fonctions au sein du CA de l'ICANN. Merci beaucoup Margarita pour cette présentation, c'était très bien. J'ai une question : les changements que vous avez présentés, que vous avez donc opérés dans les réglementations relatives aux ccTLD, maintenant vous pouvez prendre des mesures concernant les domaines qui ont été enregistrés à des fins malveillantes. Quand est-il des autres domaines, qui n'ont pas été enregistrés à des fins malveillantes, mais qui sont utilisés à des fins malveillantes ? Est-ce que là vous prenez des mesures aussi, ou c'est compliqué ?

MARGARITA VALDES

Merci beaucoup, vraiment. Nous sommes heureux de vous accueillir ici, Raul. La réponse est la suivante. Il y a ces mesures préventives et elles ne s'appliquent à tous les ccTLD. Il y a donc une frontière ténue entre les entités de mise en application et les opérateurs de registres. Parfois, il n'y a pas suffisamment de preuves pour dire que c'est un enregistrement malveillant, mais en tant qu'opérateur de registre, nous pouvons donner suffisamment d'indices aux forces de l'ordre pour qu'elles puissent enquêter pour savoir si c'est malveillant ou pas. Donc nous avons un champ d'action limité, en tant qu'opérateur de registre, mais nous pouvons communiquer avec les forces de

l'ordre pour qu'elles puissent mener une enquête s'il y a simplement une odeur de malveillance.

VANDA SCARTEZINI Maintenant nous donnons la parole à Samaneh. Veuillez vous introduire, Samaneh.

SAMANEH TAJALIZADEHKHOOB Je m'appelle Samaneh Tajalizadehkhoob, je suis directrice de la sécurité et de la stabilité de la résilience au sein de l'office de OCTO au sein de l'ICANN. C'est un plaisir d'être ici, et merci de m'inviter ici parmi ces hommes et ces femmes ici présents. Je vais vous parler aujourd'hui des idées principales sur lesquelles s'appuie notre groupe de recherche.

Quand nous parlons de la sécurité ou de l'insécurité, de l'utilisation malveillante dans l'espace du DNS, et bien ce sont les processus, les composants, les infrastructures qui ne sont pas suffisamment sécurisés. C'est des sujets qui sont abondamment débattus au sein de l'ICANN. Cela crée donc des possibilités pour les acteurs malveillants d'exploiter les vulnérabilités et de se livrer à des formes d'utilisations malveillantes du DNS. Parmi les exemples, il y a donc le hameçonnage, les logiciels malveillants, les réseaux zombies et donc les différents types de contrôles malveillants. Je ne vais pas m'approfondir dans ce domaine là. Mais donc, il y a un champ étendu d'études qui ont montré que les

défaillances sécuritaires sont causées par des incitations qui sont mal harmonisées ou des conceptions défaillantes.

Sachant cela, c'est l'idée sur laquelle s'appuie notre recherche. Alors, comment harmoniser et améliorer les incitations afin d'améliorer la sécurité et afin de minimiser l'exploitation malveillante et l'insécurité ? Il faut des indices de mesures de haute qualité. Vous les avez vus partout, et ils s'appellent les KPI, les indices de mesures. Et ces indices de mesures influent sur la prise de décision et donc la quantification de la performance sécuritaire, et donc les conceptions défaillantes peuvent conduire à l'utilisation malveillante.

Voici ce que fait mon équipe. Nous avons des données et nous nous consacrons à de nombreuses études, recherches, nous créons des indices de mesures robustes que nous pouvons présenter à la communauté., qui peuvent être utiliser pour parler des possibilités d'atténuation, pour parler des paysages qui se profilent lorsqu'il y a utilisation malveillante du DNS. Ici, vous voyez des exemples du travail que nous effectuons, et je vais vous parler de ce travail.

Voici mon équipe, l'organigramme de mon équipe. Le bureau du OCTO. Donc il y a l'équipe de recherche, l'équipe technique, les opérations et l'équipe de recherche SSR. Et donc il y a l'organigramme que vous voyez. Nos projets, vous les connaissez peut-être, le Domain Metrica. C'est celui dont on parle le plus souvent au sein de la communauté de l'ICANN. C'est le plus grand

projet, c'est une plateforme qui inclue un tableau de bord interactif, des indices de mesures sur l'utilisation malveillante. Tout ce qui est produit du point de vue de la recherche au sein de notre équipe va devenir un module au sein de Domain Metrica. Au fil du temps, nous ajouterons des modules supplémentaires. Il y a d'autres projets sur lesquels nous travaillons. Nous établissons une base scientifique et notre équipe ensuite partage cette science au sein de la communauté, et partage les résultats obtenus.

Autre aspect utile de notre point de vue, c'est une ligne de recherche consistant en la création d'une méthode pour permettre à des tiers d'évaluer si ce que nous faisons est utile, si c'est adapté aux besoins. Nous avons créé une publication universitaire, révisée par des paires, et nous avons une évaluation annuelle, s'appuyant sur l'OCTO numéro 37, donc vous pouvez l'utiliser pour les filtres, pour quantifier les cas d'utilisation malveillante du DNS et donc c'est très utile.

À ce stade, mon équipe travaille à la découverte de domaines associés, vous en avez entendu parler au cours de la semaine. C'est un sujet couvert dans les PDP à venir et cela trouve sa source dans le rapport Infermal et l'idée ici, Margarita en a parlé, dans les pratiques qu'elle nous a présentées, concernant les registres. Il s'agit d'utiliser des modèles simples pour identifier les domaines malveillants et donc ceux qui appartiennent aux mêmes groupes, où on peut dégager les mêmes tendances. Et on dégage les algorithmes similaires. Il y a des schémas similaires que nous pouvons dégager. Nous travaillons à la mesure du temps

d'atténuation. Nous mesurons le temps pendant lequel on voit le domaine jusqu'au moment où il est supprimé. Nous allons publier un rapport, et nous nous appuyons sur le travail de la communauté. Ce sujet est difficile à quantifier, car nous essayons de voir les domaines qui sont encore en activité et nous devons élaborer des techniques pour les détecter, et eux, ils ont des techniques pour pouvoir être cachés. C'est pour ça que c'est difficile de mesurer le temps où ils sont en activité, car il faut pouvoir les détecter là où ils se trouvent.

Nous examinons aussi la façon dont les domaines sont parqués, et comment ces domaines sont utilisés et comment ils diffusent les situations d'utilisations malveillantes du DNS. Notre rapport a été publié dans le contexte de l'IEEE 2023.
Sur ce, je voudrais donc conclure mon intervention et dans la mesure où nous sommes dans un espace des femmes du DNS, je voudrais me mettre à disposition pour les femmes qui s'intéressent à faire des recherches dans ce sujet, ou dans le domaine technologique d'une manière générale. Je me porte donc volontaire pour faire du mentorat ou pour répondre à des questions si je peux être utile. Merci de m'avoir donné la parole.

VANDA SCARTEZINI Merci beaucoup. Je ne connais pas très très bien ce groupe. Je ne sais pas ce qu'il en est pour les autres. J'en ai entendu parler, un peu, mais je n'ai pas participé à des discussions. Cela fait 25 ans que je suis ici, mais nous n'avons pas approfondi le sujet de ce que

fait votre groupe. C'est très important d'avoir votre présence ici. Merci beaucoup.

Mon expérience à moi est très simple. Nous sommes une association de sociétés de logiciels au Brésil. Nous avons plus de 2000 entreprises associées au sein de cette association. Mais nous n'avons pas vraiment d'implication dans le secteur de l'internet. Mais nous savons que notre population dans notre pays souffre beaucoup de ces utilisations malveillantes du DNS. Donc nous devons faire quelque chose. Nous devons agir. Les gouvernements nous disent toujours « oh vous êtes les techniciens, les gens du technique, vous devez faire quelque chose pour résoudre ce problème » parce qu'en fait personne ne comprend vraiment de quoi on parle. Et la population en général ne comprend rien quand on leur parle d'utilisation malveillante du DNS. « Qu'est-ce que c'est ça que le DNS ? Et l'utilisation malveillante du DNS ? » Nous avons aussi des mots en portugais pour désigner cela, mais le DNS c'est quoi ? On ne sait pas. Donc il faut agir. Et il faut pouvoir aussi l'expliquer aux autres. J'ai repris certaines photos de notre site et je les ai traduites en anglais, car elles sont en portugais sur notre site. L'idée c'est de pouvoir donner une idée à la population de quoi on parle. Il faut bien sûr faire attention à ce qu'il se passe dans ce domaine.

Pourquoi avons-nous créé ce site ? L'idée c'était de créer un pôle, un hub, permettant de recevoir des plaintes, les analyser et relayer ces alertes à nos partenaires au sein du Brésil, en dehors du Brésil, afin de pouvoir notamment prendre des mesures d'atténuation de

ces utilisations malveillantes où y mettre fin, parce que comme je l'ai dit à Margerita, nous n'avons pas le pouvoir de faire quoi que ce soit. Aussi, que pouvons-nous faire pour aider ? Et bien, nous pouvons faciliter ce processus. Au Brésil, nous parlons portugais, rappelez-vous. Nos voisins parlent espagnol, et l'anglais bon. Certaines personnes ne vont pas pouvoir utiliser l'anglais avec un bureau d'enregistrement ailleurs dans le monde. On peut passer à la diapo suivante.

Ça c'est une autre illustration qu'on utilise sur notre site, pour vous expliquer un peu ce qu'est l'utilisation malveillante du DNS. Ensuite, comment notifier, comment informer de ces cas ? Alors, nous on ne parle pas d'utilisation malveillante. On parle de cybercrime, qui est le même en anglais, en portugais et en français. Et on se sert de ce mot pour informer les gens qu'ici on parle de criminalité, et qu'ils doivent faire attention. Et toutes les alertes, on les reçoit à cette adresse mail là que vous voyez à l'écran. Et il y a beaucoup de webinaires qui sont donnés afin d'expliquer aux gens la façon de procéder, et on leur demande toujours de nous renvoyer le premier e-mail qu'ils ont reçu. On ne leur demande pas de nous envoyer leur carte d'identité, non. On leur demande le premier e-mail qu'ils ont reçu pour qu'on puisse analyser, comprendre le problème. Et c'est très difficile de faire ça avec la population en général. Quand on s'entretient avec des personnes qui ont plus d'expériences dans le milieu technique, ça va, ce n'est pas si difficile. Mais par contre, avec la population, avec le citoyen lambda, c'est très difficile. Il faut vraiment tenter de leur faciliter la

tâche au maximum, afin qu'ils nous envoient les bonnes informations de façon correcte, afin qu'on puisse traiter ces problèmes. Ensuite, si ces personnes veulent savoir ce qu'il s'est passé par la suite, assurer le suivi, on peut leur demander leur nom et leur envoyer des e-mails par la suite pour les informer de ce que nous avons fait.

Notre association coopère avec des partenaires en dehors de notre pays, avec des bureaux d'enregistrement, d'autres opérateurs de registres ccTLD afin de les aider aussi pour toutes les mesures d'atténuation qu'il faut prendre pour atténuer, justement, tous les problèmes dans leurs environnements. Ce service est ouvert à tous, accessible à tous. Pour le moment, il n'est disponible qu'en portugais, mais nous allons bientôt le rendre disponible en espagnol afin qu'il soit disponible en Amérique Latine partout, et bien sûr c'est un service gratuit. Voilà, c'est notre façon de contribuer. Notre association appartient aussi à l'unité constitutive des entités commerciales. Voilà comment nous pouvons coopérer. Et je voulais partager cela avec vous, parce que vous pouvez faire un copier-coller. Vous pouvez émuler nos stratégies pour atténuer ces problèmes que tout le monde rencontre. Merci beaucoup.

CHERYL LANGDON-ORR Alors Mesdames et Messieurs, le temps est notre ennemi, comme c'est toujours le cas, et sur base de ce qu'à dit Samaneh, j'espère bien prononcer votre prénom, nous avons donc de Samaneh une

offre très généreuse de coopération. Peut-être que l'on pourrait aussi prendre note de touts les questions que vous auriez à poser à nos panélistes aujourd'hui, et nous nous assurerons de relayer vos questions à nos panélistes, et mieux encore : nous nous assurerons qu'elles vous répondront. Mais nous allons devoir lever cette séance, car nous allons devoir libérer nos fabuleuses interprètes, et nous voudrions aussi libérer l'équipe technique qui a eu une très longue journée et qui va avoir envie de tout débrancher, d'ici à bientôt. Alors maintenant, nous aimerions prendre une photo. Alors je sais que vous avez toutes et tous un autre endroit où aller aujourd'hui, donc on va faire ça rapidement. Aussi rassemblez-vous de façon à ce qu'on puisse prendre une photo, pour l'ajouter à notre collection photo des femmes du DNS.

Merci beaucoup à toutes et à tous d'avoir participé à cette séance. Je voudrais vraiment vous remercier pour votre présence. La photo de famille se fera à la réception dans le hall d'entrée. Les photographes vous attendent, donc quittez le bâtiment de façon ordonnée, et rapprochez-vous de nous. On espère que les photographes prendront cette photo rapidement, et que cela ne prendra pas trop de temps. Donc la photo de famille se fera dans le hall d'entrée, dans le lobby. Merci.

[FIN DE TRANSCRIPTION]