FR

ICANN83 | Forum de politiques – ccNSO : DASC Online Escroqueries et crimes financiers
Mercredi 11 juin 2025 – 13h45 à 15h00 CEST

CLAUDIA RUIZ

Bonjour et bienvenue à cette séance de la ccNSO sur le DASC, je suis responsable avec mes collègues de la participation à distance pour cette séance.

Cette session est enregistrée et régie par les normes de comportement attendues de l'ICANN ainsi que les règles anti-harcèlement de la communauté de l'ICANN.

Lors de cette séance, les questions et commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre questions et réponses. L'interprétation sera assurée en anglais, français et espagnol.

Si vous souhaitez prendre la parole, veuillez lever la main dans Zoom, lorsque vous serez appelé, les participants à distance auront le droit d'activer leur micro. Les participants sur place utiliseront un micro physique pour parler. Veuillez donner votre nom pour l'enregistrement et la langue dans laquelle vous allez vous exprimer si ce n'est pas l'anglais. Et veuillez parler à un rythme raisonnable pour permettre aux interprètes de travailler.

Je vous donne la parole.

NICK WENBAN-SMITH Merci, Claudia. Je suis Nick de NOMINET.UK de ccTLD et je suis le président du comité permanent de la lutte contre l'utilisation malveillante du DNS.

Aujourd'hui nous allons parler de ce thème en nous basant un petit peu sur ce qui a été dit pendant les réunions préalables et nous allons essayer de parler des priorités pour les ccTLD du monde entier.

Je suis très content d'être ici avec vous et de présider ce panel d'experts et je pense que le contenu va être très intéressant. L'objectif de cette séance est d'être interactive, s'il y a des questions, nous les suivrons et les prendrons dans la salle Zoom, le personnel me le dira, j'en suis sûr.

Nous avons un ordre du jour assez rempli. Je vais présenter rapidement les différents panélistes. Nous avons Gabriel Andrews du bureau de recherche, bureau fédéral.

GABRIEL ANDREWS Bonjour, je travaille pour le FBI et aussi pour l'ICANN.

NICK WENBAN-SMITH Merci. Keith ?

KEITH DRAZEK Bonjour, je travaille pour Verisign et je suis responsable au sein de la communauté de l'utilisation malveillante du DNS et du programme d'atténuation. Je travaille aussi pour l'équipe de politique des parties prenantes de l'ICANN. Je suis très heureux d'être ici. Vous me connaissez, j'ai travaillé pour plusieurs compagnies, pour .US, et je suis là de nouveau et j'en suis très heureux.

NICK WENBAN-SMITH Mon ? Pourriez-vous vous présenter ?

MON PEREZ Bonjour, je suis responsable technique de SGNIC, je suis responsable des opérations pour le registre de noms de domaine de SG et je suis également responsable de tout ce qui est le système de gestion de la lutte contre l'utilisation malveillante du DNS

NICK WENBAN-SMITH Merci beaucoup. Bruce ?

BRUCE TONKIN Bonjour, je suis de .AU, extension géographique .AU.

NICK WENBAN-SMITH Merci. Mon est à Singapour, il nous suit en ligne. Comme vous le voyez, les photos des panélistes datent d'avant le Covid. Merci.

Maintenant, pour présenter un peu cette séance, elle vise à explorer le thème des fraudes en ligne, des fraudes financières et surtout l'intersection entre l'utilisation malveillante du nom de domaine et différents délits, les délits techniques et les délits qui ont un impact sur la société. Par conséquent, nous allons parler des niveaux de problèmes et voir quelles sont les approches, les défis qui restent à résoudre.

Prochaine diapositive s'il vous plait.

Un premier aperçu de ce qu'est le comité permanent sur l'utilisation malveillante du DNS, le DASC. Nous travaillons au niveau national, chaque ccTLD travaille au niveau national. Nous sommes ici pour promouvoir la compréhension, la sensibilisation, nous voulons créer un dialogue constructif et, finalement, l'objectif est de diminuer la quantité d'utilisation malveillante du DNS concernant les registres ccTLD pour que tout le monde puisse atteindre son objectif dans ce sens.

Voilà un petit peu la situation telle qu'elle est, en 2022, 2024, nous avons fait une enquête auprès des ccTLD et voilà les résultats intéressants. Il s'agit d'une bifurcation ici en termes des politiques de l'ICANN. Les gTLD sont toujours sous la responsabilité de la politique de l'ICANN, mais quand on fait des enquêtes, on se rend compte que beaucoup de ccTLD n'ont pas vraiment tenu compte de tout cela et ne font pas de différence entre les différents types d'abus et on considère tout cela comme des abus et utilisations malveillantes. Pourtant il y a des contenus criminels, des fraudes,

des questions sur lesquelles on peut agir au niveau légal, des questions pour lesquelles l'opérateur de registre doit intervenir.

Donc je voudrais me rapporter à notre réunion de Kigali. Nous avons entendu parler, par exemple l'opérateur de registre du Nigéria qui nous a parlé du problème qu'ils avaient concernant les fraudes de cryptomonnaie qui visaient les consommateurs les plus vulnérables de ce pays. Au Royaume-Uni, nous avons aussi des problèmes de fraude qui représentent 40 % des délits. C'est un niveau élevé, 80 % sont des délits concernant les paiements qui viennent des réseaux sociaux, des sites internet qui sont faux. Nous avons ici vraiment quelque chose d'important qui est sous la responsabilité des registres ccTLD.

Bien sûr, il y a beaucoup de points communs entre l'utilisation malveillante du DNS, le hameçonnage, les différents niveaux d'abus dans le monde entier. Les hameçonnages, les imitations d'email, les délits financiers, nous en avons parlé lors de notre dernière réunion à Seattle.

Par conséquent, nous allons passer directement aux débats. Je vais d'abord donner une définition de ce qu'est une fraude, invitation frauduleuse, demande ou notification, une offre pour obtenir une information ou de l'argent ou des bénéfices financiers en trompant la personne.

Prochaine diapositive.

Ici, notre séance d'aujourd'hui de l'ICANN 83 vise à approfondir le travail réalisé jusqu'à maintenant dans les réunions précédentes et nous souhaitons continuer à travailler avec les parties prenantes de la communauté.

Nous allons faire une petite enquête avant de continuer. Par conséquent, nous allons faire 2 minutes de pause, c'est quelque chose que nous faisons bien au sein de la ccNSO, nous faisons des enquêtes interactives pour savoir vraiment comment vous suivez, cela aide les personnes qui ne parlent pas l'anglais comme langue natale et cela permet de savoir si tout le monde nous suit.

Alors, dites-moi si vous pouvez afficher la question. Prochaine diapositive. Voilà. La question est assez facile : dans quelle mesure votre opérateur de registre ou votre registre est préparé à détecter des abus de domaine liés aux crimes financiers ? Vous avez la possibilité de répondre maintenant.

Ce n'est pas une enquête scientifique, c'est juste pour voir un petit peu où on en est et connaitre l'échelle du problème et comprendre le problème.

Maintenant je vais donner la parole à Gabe qui va faire sa présentation.

GABRIEL ANDREWS Merci. Prochaine diapositive. Merci.

À Seattle nous l'avons dit, on a dit que les délits liés à l'internet au niveau annuel reporté par le FBI étaient de ce niveau, vous le voyez ici sur l'écran. Donc je remercie l'ICANN de me donner la parole.

Ici vous voyez le portail du centre de plaintes liées aux crimes ou délits sur internet. Ici nous avons un portail qui nous aide vraiment à savoir comment cela fonctionne, à avoir toutes les ressources, à analyser les cas et à aider les victimes. Cela nous donne des statistiques intéressantes au niveau annuel et pour travailler.

Je veux d'abord reconnaitre que je suis juste un agent d'un pays, mais nous avons ces chiffres et nous recevons des plaintes de 200 et quelques pays du monde entier que vous voyez ici affichés sur l'écran. Le Royaume-Uni a été responsable de 100 mille plaintes, par exemple. Vous voyez que le cyberdélit est quelque chose de mondial. Je pense que quand on parle de statistique des États-Unis cela représente vraiment ce qu'il se passe dans le monde entier.

Prochaine diapositive.

Nous comptons le nombre de plaintes reçues et nous essayons de voir les pertes qui sont associées avec chaque catégorie de plaintes et de délits et j'ai souligné ici quelques plaintes sur la gauche. Vous voyez le hameçonnage est responsable du plus grand nombre de plaintes, ce qui est logique, car il a lieu en permanence et, comme l'a dit Nick tout à l'heure, c'est le vecteur d'intrusion principal, c'est comme cela que les délits sont perpétués.

Ensuite, vers la droite, vous avez les types de pertes qui ont eu lieu, des fraudes dans le domaine de l'investissement, cryptomonnaie et autre. Le cas du Nigéria que nous avons entendu. Donc c'est un fléau grave qui est responsable de plus de 6 milliards de dollars et demi de pertes aux États-Unis en 2024, donc vous vous rendez compte que c'est important, avec des suicides de victimes et des pertes des victimes humaines aussi.

Ensuite, nous avons différents types de compromis, emails d'affaires, un autre cas important. Et je sais que ce n'est pas exactement des fraudes, mais c'est quelque chose qui peut avoir un impact important sur la vie d'une personne.

Ici vous voyez le hameçonnage, le système typique, une personne qui prend votre identité, qui fait un virement et voilà, ce type de problèmes qu'on a depuis l'année 2015.

Et, ici, si vous regardez, je ne sais pas si c'est sur cette diapo ou une autre… Voyons, pouvez-vous cliquer une fois de plus pour voir ? Voilà, c'est cela.

Vous voyez ici que le sujet réel était l'adresse email, il s'agissait d'un enregistrement d'un nom de domaine et ici, en tant qu'enquêteur, je voulais savoir ce qui était disponible sur ce nom de domaine. J'ai fait une recherche sur WHOIS et une des raisons pour cela est que je voulais savoir où je pouvais envoyer toute la procédure juridique, dans un autre pays, où est-ce que nous allions devoir travailler.

La procédure juridique peut prendre un certain temps avant d'être entamée. On nous demande donc quels sont les autres noms de domaine que ces criminels ont enregistré. Et nous savons que c'est une douzaine, peut-être même plusieurs douzaines de domaines. Et mon travail, dans le cours de cette enquête, est que je veux que les victimes potentielles soient ciblées par ces criminels, donc je n'ai peut-être pas le temps de suivre une procédure juridique qui peut durer des semaines, mais si je peux trouver sur WHOIS des coordonnées, je vais pouvoir empêcher d'autres préjudices.

Diapositive suivante.

De façon similaire, avec le rançon-logiciel, j'ai échangé avec notre agence sœur CISA, et je voudrais souligner que c'est une catégorie de criminalité complètement différente. Ici, ce qu'ils font, c'est très similaire à ce que j'ai décrit. Nous essayons d'empêcher ces crimes, il y a des chercheurs de cybercriminalité qui recherchent les rançons-logiciels qui sont connus. Et on sait que quand une nouvelle victime est identifiée au cours des prochaines 72 heures, par exemple, il y aura ce rançon-logiciel qui sera déployé contre cette victime. Les chercheurs vont nous contacter, CISA ou le FBI et ils vont nous dire : il y a une nouvelle victime qui a été détectée, on a détecté son IP et la procédure se déclenche. Donc, eux se fient aussi aux données publiques. C'est très important de pouvoir accéder à ces données. Je crois que c'est 8,5 milliards de dollars qui ont été empêchés, en termes de pertes, avec ces rançons-logiciels.

Diapositive suivante.

La fraude à la cryptomonnaie et dans ce domaine. Vous avez entendu parler du Nigéria et aux États-Unis c'est l'une des principales causes de préjudices financiers, plus de 6 milliards de dollars.

Diapositive suivante.

Ici, je crois que chacun dans cette salle a potentiellement été ciblé par ce genre de chose, c'est un message que l'on reçoit Whatsapp ou autre, et quelqu'un prétend être un ami ou une connaissance. Donc il y aura un échange qui va être entamé et il s'agira de développer la confiance de l'interlocuteur. Ce sont les fausses plateformes de trading, les faux comptes de trading, on vous montre de fausses informations, avec des taux d'intérêt qui ne sont pas réels.

Ici, vous voyez une plateforme de cryptomonnaie, on vous montre des données qui semblent vraiment réelles.

Diapositive suivante.

Les criminels vont enregistrer des centaines de domaines pour promouvoir ces fausses informations aux victimes. Si vous voyez que dans vos ccTLD il y a des enregistrements groupés, c'est peut-être ce genre de choses. Ils vont utiliser ces ccTLD. C'est un volume considérable et la difficulté pour les enquêteurs c'est que les opérateurs de registre qui sont utilisés ne sont pas situés sur le même lieu que les criminels.

Quand on utilise des informations qui sont dans le domaine public, comme sur Google ou autres, on peut faire des recherches en quelques minutes. Donc quand on veut suivre une procédure judiciaire avec un mandat de perquisition, cela peut prendre du temps. Et quand on veut faire une enquête transfrontalière, la procédure est longue, six à douze mois, c'est ce que cela peut prendre, d'après mon expérience passée.

Donc quand on a la possibilité d'accepter des données provenant de WHOIS, notre travail peut être grandement facilité.

Dernière diapositive.

C'est pour un récapitulatif rapide. Les données WHOIS sont très utiles pour intervenir à travers le monde, pour accélérer la procédure, car sinon la procédure juridique est longue. Les agences de sécurité publique utilisent WHOIS et les opérateurs de plateformes de cryptomonnaies frauduleuses enregistrent leurs sites de façon groupée pour promouvoir leurs plateformes frauduleuses.

Je vous remercie de votre attention, j'espère que mon intervention vous aura été utile.

NICK WENBAN-SMITH Merci, Gabe. Y a-t-il des questions immédiates que vous souhaiteriez poser ? On a l'impression que ce sont les gTLD qui sont impactés, mais cela concerne aussi les ccTLD. Et avec tout le respect que je vous dois, je ne reconnais pas l'autorité des États-

Unis, si je vois quelque chose qui me provient du FBI je ne vais pas forcément le mettre à la poubelle, si je vois une information qui provient de cet organisme. Mais il y a des procédures pour les ccTLD si l'on voit que ce sont des données d'enregistrement qui sont de toute évidence frauduleuses, il y a une procédure qui peut être suivie. Nous pouvons en reparler.

Passons à Keith, à ma gauche.

KEITH DRAZEK Merci beaucoup. Je voudrais parler du forum d'infrastructure internet qui est une nouvelle initiative. Et je voudrais vous donner un contexte et vous dire pourquoi nous soutenons cette initiative parmi d'autres.

En 2022 les bureaux d'enregistrement et registres gTLD ont dit qu'il fallait traiter du sujet de l'usage malveillant du DNS. Il y a eu des discussions pendant 10 ans sur la question de l'utilisation malveillante du DNS au sein de l'ICANN, nous avons considéré qu'il fallait faire quelque chose et nous nous sommes impliqués auprès de l'ICANN et nous avons proposé de prendre des mesures dans un cadre contractuel pour l'utilisation malveillante du DNS et nous avons défini qu'il s'agissait de hameçonnage de réseaux zombie, de courriers indésirables notamment. Donc définir cela dans nos contrats est important et nous nous sommes rendu compte qu'il y aurait de la pression exercée sur l'ICANN.

Vous ne le savez peut-être pas, les statuts de l'ICANN l'empêchaient de s'impliquer dans tout ce qui est contenu et il a été nécessaire d'établir un canal multipartite pour inclure les contenus, mais en dehors de l'égide de l'ICANN.

Plusieurs bureaux d'enregistrement et registres gTLD se sont réunis pour parler de la nécessité de créer ce forum d'infrastructure internet. Google, Cloudfare sont parmi les 6 entreprises qui ont considéré que notre travail était utile et les opérateurs d'infrastructure internet ont décidé de parler de la façon dont les opérateurs d'infrastructure internet peuvent prendre des mesures pour atténuer ces problèmes de façon plus énergique.

C'est une initiative qui a réellement débuté l'année dernière, nous avons eu notre première réunion en février de cette année, il y avait 53 participants représentant 38 organisations sur une durée de deux jours de réunion. Cela a été très bien reçu et les 6 entreprises qui se sont réunies pour cette initiative travaillent étroitement avec l'organisme que représente Bertrand de La Chapelle et l'un des principaux acteurs de l'organisation de ce forum. Il y a aussi la coalition d'infrastructure internet qui est basée aux États-Unis. Donc il y a ce groupe qui forme le noyau des participants à ce forum.

Donc, en sortant de cette réunion d'Amsterdam, ce qui était important c'est de valider que cette entreprise est de grande valeur, surtout pour les fournisseurs de service sur le cloud, notamment, qui ne participent pas forcément à l'espace de

l'ICANN, mais ils souhaitent s'impliquer dans la couche liée au contenu. Il s'agit pour nous de déterminer comment nous pouvons travailler ensemble de façon collaborative, partager des informations, identifier des sujets concrets pour atténuer la cybercriminalité et vraiment atténuer les préjudices.

Nous avons identifié 4 pistes de travail, une sur les questions juridiques et règlementaires pour inclure l'implication DSA et donc il faut connaitre les problèmes rencontrés par les clients, tout cela dans le cadre des règles RGPD. Et la deuxième piste, ce sont les questions opérationnelles, l'automatisation, comment nous élaborons les systèmes qui nous permettent le routage des signalements des utilisations malveillantes et comment communiquer de façon plus efficace pour vraiment gérer de façon plus immédiate les préjudices.

Deux autres pistes consistent à l'imagerie non consensuelle, notamment. Il s'agit vraiment du rôle des notificateurs de confiance. La dernière piste est le hameçonnage plus. Comme Gabe l'a dit, le hameçonnage est l'un des principaux vecteurs de fraudes et il donne suite à de nombreux autres abus.

Donc c'est une initiative qui est vraiment enthousiasmante et nous cherchons à élargir notre effectif et notre participation, nous souhaitons une participation accrue et maintenir un équilibre entre les opérateurs DNS traditionnels, mais aussi impliquer les hébergeurs, les hôtes.

Et il faut savoir que c'est une initiative qui est menée par les membres du secteur, l'industrie et tous ceux qui sont concernés et préoccupés par l'usage malveillant du DNS. Et il faut étendre notre travail pour aussi impliquer les différentes parties prenantes, impliquer des groupes qui ont de l'expertise pour passer aux étapes suivantes, il faut faire progresser notre travail dans le cadre d'une implication multipartite.

Voilà, je m'arrête ici.

NICK WENBAN-SMITH Merci, Keith. Une des raisons pour lesquelles nous avons voulu introduire cette présentation ici dans notre réunion, c'est parce que nous savons tous que le fait d'agir au niveau du nom de domaine est quelque chose qui ne parait pas toujours d'aborder et régler le contenu du problème. Donc, aller auprès du site internet, obtenir des résultats et arriver à avoir vraiment une action efficace, c'est difficile.

Nous savons que ce que l'on peut faire auprès des opérateurs de ccTLD ne va pas empêcher que certains noms de domaine continuent à exister. Donc je pense que cette perspective est intéressante et il faut s'en souvenir pour de futures discussions liées au contenu, cela peut être très utile.

Nous allons passer à Mon Perez de Singapour, qui va nous parler d'une initiative pour lutter contre les escroqueries en ligne.

MON PEREZ

Merci. Prochaine diapositive. Je vais d'abord vous mettre en contexte, un petit peu, nous savons tous qu'il existe des pertes financières et de graves dommages et nous avons géré un rapport dans ce domaine et une recherche à Singapour. Et on a constaté qu'il y avait eu plus de 8000 tentatives de hameçonnage en 2022, aucune d'entre elles n'a eu lieu ici à Singapour, mais 80 % de ces tentatives ciblaient des banques et des services financiers.

Ces abus nous ont intéressés, intéressent SGNIC. Nous avons divisé tout cela en plusieurs catégories. Dans la première, vous voyez les utilisations malveillantes du DNS qu'ICANN a classé parmi le hameçonnage, les dévoiements, botnet, etc. Ensuite il y a les utilisations malveillantes qui inquiètent et préoccupent SGNIC. De nouveau vous avez ici une liste avec vol d'identité, fausses identités, pornographie, etc. Et dans la troisième catégorie, vous avez les vérifications supplémentaires que SGNIC a faites pour essayer de prévenir ces utilisations malveillantes.

Voilà les mesures de prévention que nous avons mises en œuvre au niveau de SGNIC. D'abord il faut vérifier l'identité et s'assurer que les enregistrements de noms de domaine ont fait des vérifications en utilisant le SINGPASS, ce qui réduit le vol d'identité. Ensuite le blocage de registre, il s'agit d'une fonction de sécurité qui est gratuite pour aider les titulaires de nom de domaine de .SG à atténuer le risque de vol de nom de domaine ou de modification non autorisés. Et, ensuite, les systèmes de gestion des utilisations malveillantes. Il s'agit d'un système interne qui permet de contrôler tout ce qui est utilisation malveillante ou les actions

malveillantes sur les sites internet et d'alerter les parties prenantes pour qu'elles prennent les actions nécessaires.

Je vais vous parler plus des mesures que nous avons prises dans le cadre de ces utilisations malveillantes. Nous essayons détecter et suivre les abus des noms de domaine dans le nom du hameçonnage, informations d'enregistrement incorrectes ou que nous pouvons soupçonner, utilisation de DNS frauduleux. Et nous essayons de notifier les parties prenantes, titulaires de nom de domaine, bureau d'enregistrement, le fournisseur d'hébergement pour des actions. Et ensuite, si nous confirmons le problème, nous allons collaborer avec les différentes parties prenantes, une fois que nous les avons notifiés et nous collaborons avec SINGCERT pour fournir des opinions d'experts de façon à détecter ce type d'actions malveillantes.

Et puis il y a un rôle commercial qui fournit suffisamment de données pour détecter des contenus d'utilisation malveillante dans ce cadre.

Ici nous avons des systèmes de gestion des abus pour les enregistrements qui nous paraissent incorrects ou que nous pouvons soupçonner de l'être. Ici nous allons vérifier le numéro d'enregistrement de la compagnie, si cela correspond au numéro d'enregistrement de la compagnie, si cela correspond au nom de la compagnie dans la base de données. Et en fonction du nom de la compagnie, nous allons comparer tout cela et vérifier si

l'enregistrement a été fait correctement ou s'il y a de bonnes raisons de soupçonner une fraude.

Ici nous avons un système de gestion d'utilisation malveillante. Dans le cas de hameçonnage, cela fournit une vision des menaces ou des attaques courantes et de tout ce qui peut être ciblé au niveau des applications.

Ici vous voyez un nom de domaine et les tendances des utilisations malveillantes des noms de domaine avec les différentes fraudes possibles.

Que se passe-t-il et quels sont les résultats de ces efforts faits par SGNIC ? Au début, nous n'avions aucun incident rapporté concernant le vol de nom de domaine ou le piratage de nom de domaine. Ensuite nous avons mis en place un taux de résolution et de mesure pour conserver 80%de cas résolus par mois. Ensuite, nous avons été bien informés pour les menaces qui pouvaient apparaitre ou les menaces qui existaient en permanence.

Nous avons commencé à travailler en 2010 et en juillet 2012 une plateforme d'hébergement sur le web qui été connue a été exploitée et nous avons pu voir environ une centaine de noms de domaines de .SG utilisés pour le hameçonnage. Cela nous a permis de réagir rapidement, nous avons contacté le fournisseur d'hébergement que nous avons identifié à travers SGNIC et nous avons coordonné avec les gestionnaires et le problème a été résolu quelques heures après.

Une autre tendance que nous avons constatée concerne les bibliothèques open source qui sont compromises et nous essayons de travailler avec les acteurs qui menacent ces systèmes et nous avons par exemple pu injecter un code. Et, depuis, cette bibliothèque qui était très utilisée, avec une quarantaine de noms de domaine exclus qui étaient affectés, nous avons notifié chacun des titulaires de nom de domaine et nous avons pu corriger la situation.

Quels sont les défis que nous devons affronter dans le domaine de l'atténuation des risques de ce type ?

D'abord il faut éduquer et sensibiliser les titulaires de nom de domaine. Beaucoup ne savent pas que faire et certains fournisseurs d'hébergement ne savent pas non plus comment corriger le problème. Ensuite, on constate que souvent les gens ne savent pas où trouver les informations concernant ces problèmes. Ensuite, retarder la résolution, certains titulaires de noms de domaine ont besoin de temps pour contacter leur fournisseur, et certains fournisseurs mettent du temps pour faire les corrections nécessaires.

Et, finalement, une difficulté à annuler les domaines qui représentent des risques élevés. Par exemple il y a eu un cas dans lequel on avait un domaine et le personnel technique avait l'impression que c'était un domaine malveillant, mais comme il n'était pas sûr, ils n'ont pas voulu fermer ce site. Il a fallu dans ce

cas-là, par exemple, que nous notifiions la victime et que nous lui disions que nous devions fermer ce site.

Quel est l'impact de notre stratégie d'atténuation sur notre système ?

D'abord nous maintenant un niveau d'utilisation malveillante assez bas, nous avons 5 cas confirmés par mois dans les situations normales. Ensuite, nous avons pu sensibiliser la communauté en fonction de tout ce travail. Nous avons pu créer une sensibilisation pour toutes les personnes concernées de façon à ce que chacun puisse apprendre à reconnaitre des menaces et à mettre en place des protections pour leur site ou leur domaine. Ensuite, nous avons pu maintenir une confiance envers .SG, notre espace de noms continue à être considéré comme sûr et digne de confiance par le public et les entreprises.

Finalement, nous avons augmenté la confiance du gouvernement envers notre travail, nos efforts pour gérer et garantir le travail de .SG, cela a donné des résultats, SGNIC est digne de confiance et nous savons que nous pouvons lutter contre les crimes et les délits financiers et que nous sommes reconnus dans ce sens.

Je vous remercie, j'en ai terminé.

NICK WENBAN-SMITH

Merci beaucoup. Bien, nous avons encore quelques questions. Je voudrais d'abord passer à la présentation suivante, celle de Bruce, et ensuite nous passerons aux questions, de façon à respecter

notre programme. Mais n'oubliez pas de noter vos questions et nous les poserons une fois que nous aurons entendu le dernier intervenant. Merci.

BRUCE TONKIN

Merci, Nick. Ce que je trouve utile dans cette séance, nous en avons parlé dans les précédentes aussi, nous avons parlé du hameçonnage, des logiciels malveillants, nous nous concentrons sur cela déjà depuis plusieurs années. Et nous avons maintenant des sites web qui sont compromis plutôt que des noms de domaine enregistrés. Ce sont donc les sites même qui sont hameçonnés.

Nous nous rendons compte que dans le contexte australien, c'est toute une économie numérique qui existe, toutes nos transactions sont électroniques, j'utilise très peu d'espèces. Auparavant, les escroqueries se déroulaient dans des établissements tels que des bars ou autres, dans le monde numérique, l'escroc ne se trouve pas à proximité de l'endroit où vous êtes, ce sont donc des opérations qui sont complètement délocalisées.

Donc l'axe de concentration a changé, c'est très difficile à éliminer, mais vous pouvez essayer de perturber les activités malveillantes.

Le gouvernement australien a déterminé qu'il faut se concentrer sur l'aspect financier, l'aspect télécommunication. On a parlé tout à l'heure de ces plateformes, des contacts par téléphone, par SMS, donc il y a tous ces éléments et il faut travailler de façon collaborative et chacun dans l'écosystème a un rôle à jouer.

Nous avons maintenant un centre anti-escroquerie financé par le gouvernement. Voilà les diapositives.

L'autre activité qui est intéressante dans notre environnement concerne les jeux de hasard, les jeux d'argent. Par exemple pour le football et vous ne vous rendez pas forcément compte que vous êtes victime d'une escroquerie.

Diapositive suivante. Une autre encore.

En Australie, nous avons des définitions, donc une escroquerie doit impliquer une tromperie et si elle réussit, la victime subit un préjudice. Et, souvent, cela peut être des entreprises et l'escroquerie va se dérouler dans le domaine d'activité.

Nous obtenons des informations de nombreuses sources et nous pouvons signaler qu'il y aura une escroquerie utilisant un nom de domaine.

Diapo suivante.

Voilà le cadre créé par le gouvernement australien, on nous indique les mesures à prendre, premièrement. Il faut avoir des processus pour combattre les escroqueries. Il faut prendre des mesures raisonnables, il faut effectuer des vérifications au moment de l'enregistrement. Nous vérifions tous les enregistrements qui viennent des bureaux d'enregistrement et nous vérifions la légitimité de tous les acteurs.

Il y a eu, au cours des discussions sur les politiques, dans les réunions GNSO, le fait qu'il faut examiner les noms qui doivent être

vérifiés pour déterminer s'ils sont légitimes. Il faut donc prévenir, détecter, perturber.

J'ai entendu plusieurs interventions cette semaine où on nous indique que ces escrocs enregistrent des groupes de noms, des centaines de noms. Et une fois qu'ils sont arrivés à leurs fins, ils se débarrassent de leurs domaines, mais ils continuent ensuite à enregistrer de nouveaux noms. Et une fois qu'on les a détectés, ils passent à une autre extension géographique. Je pense que quand on détecte un escroc, à ce moment-là il est déjà passé à une autre victime.

Il a la riposte aussi, comment riposter, comment signaler.

Diapositive suivante.

Il y a une catégorie que l'on classifie comme étant malveillante, ce sont de fausses informations. Il y a des informations qui peuvent avoir été volées, par exemple un permis de conduire, un passeport qui ont été volés. Cela peut être facile à détecter. Mais les escrocs sont plus malins et ils procèdent par d'autres voies.

Ce que nous avons, notre avantage, c'est que, comme en Chine ou à Singapour, il y a des règles qui indiquent que le nom de domaine doit être lié au pays. Quand nous voyons un nom de domaine lié à une escroquerie financière, nous ne supprimons pas le site en raison de la fraude, mais en raison de fausses informations. Ainsi, il n'est pas nécessaire d'avoir une injonction du tribunal, on peut

supprimer ce nom en raison de la diffusion de fausses informations.

Ensuite il y a les sites web qui sont compromis. Il y a des sites où l'on peut faire des commentaires, mettre des appréciations et les pirates utilisent ce type de sites et ces sites sont souvent piratés. Et dans ces situations nous ne supprimons pas le nom de domaine, car nous ne souhaitons faire fermer l'entreprise, nous contactons le bureau d'enregistrement ou le titulaire du nom de domaine. Et, en général, ils sont surpris.

Il faut faire de la pédagogie parce que quand le titulaire de domaine est contacté, il ne sait pas qui héberge ce site, donc il faut comprendre l'écosystème, il faut savoir qui contacter pour apporter les corrections nécessaires plutôt que de supprimer le site.

Diapositive suivante.

J'utilise le même cadre australien. Au niveau du gouvernement, nous faisons des suivis, nous rationalisons, nous améliorons nos processus de validation, nous détectons et nous recherchons des tendances, des schémas. Par exemple pour les sites de jeux, nous faisons des recherches sur Google pour trouver d'autres domaines qui s'alignent sur ces tendances. Et nous supprimons des groupes entiers de noms. Et nous essayons de perturber. Si un domaine a été signalé, vous en aurez peut-être déjà des centaines au sein du registre.

Nous essayons d'être réactifs, nous travaillons avec les forces de l'ordre, mais nous recevons des informations des forces de l'ordre à concurrence de 1 % seulement, c'est 1 % des informations que nous recevons. Mais nous interagissons avec eux dans la mesure du nécessaire. Ensuite il s'agit de faire des rapports, de signaler. Évidement on ne doit pas partager des informations confidentielles, mais il est important de partager des informations. Quand nous détectons un problème, une fraude, en général la fraude se produit ailleurs. Il faut une coordination entre les bureaux d'enregistrement et entre les entreprises d'hébergement et il faut donc pouvoir détecter ces mauvais acteurs.

Merci.

NICK WENBAN-SMITH

Il y a beaucoup d'informations, c'est un phénomène de très grande ampleur, il coûte cher aux citoyens de chaque pays et cela a un impact sur les opérateurs de registre. C'est un coût considérable pour les consommateurs et des pertes considérables. Il y a la confiance, la réputation qui sont compromises dans un monde de plus en plus numérisé et il faut que les gens puissent avoir confiance quand ils se rendent sur internet, en ligne.

Je sais qu'il y a des questions qui sont posées. Il nous reste environ un quart d'heure. Nous voyons Olga et si vous êtes en ligne, levez la main sur Zoom.

OLGA CAVALLI

Merci pour ces interventions. J'ai une question pour le représentant du FBI. Le montant des pertes que vous avez mentionné dans votre intervention, est-ce que ce sont les victimes qui vous signalent ces chiffres ou vous avez une méthode de calcul pour estimer le préjudice subit ? Vous pouvez nous expliquer cela ?

GABRIEL ANDREWS

Merci pour la question. Ces chiffres sont les chiffres qui nous sont signalés. Donc quand nous sommes déjà dans une procédure judiciaire, quand la justice a été saisie, nous recevons des informations sur le préjudice subit par les victimes. Mais, parfois, les victimes souhaitent exagérer, par exemple il y a des gens qui disent qu'on leur a demandé de payer 5 millions de dollars pour récupérer leurs données, mais en général, ce sont les victimes qui signalent les chiffres.

NICK WENBAN-SMITH

Question suivante ?

HILDE THUNEM

Merci, je suis du registre de Norvège. Je vais commencer par une première question au représentant du FBI. Les recherches récentes indiquent que 80 % du hameçonnage vient de noms de domaines détournés, 20 % d'enregistrements malveillants. Donc je dirais que l'enregistrement malveillant n'atteint presque rien dans certains cas, c'est seulement des noms de domaine détournés. Quand vous présentez ces tendances, est-ce que vous faites une différence

entre ce qui est un site détourné, un domaine détourné ? Parce la personne derrière le domaine est finalement une victime et vous n'allez pas entrer en contact avec l'opérateur de registre, j'imagine.

GABRIEL ANDREWS

C'est une question importante. La réponse, en fonction des circonstances, va changer. La réponse raisonnable dépend du résultat escompté.

Une des premières choses que l'on essaye de faire quand on constate une fraude c'est savoir quelle est l'infrastructure, qui sont ces personnes malveillantes et, ensuite, qui est le client légitime. Donc des fois on a un site internet détourné et on a du mal à se rendre compte qui est qui. Il faut d'abord atténuer les dommages et ce serait raisonnable d'identifier d'abord l'enregistrement malveillant, voir qui est le bureau d'enregistrement, l'opérateur de registre et travailler de cette manière. Mais on n'a pas toujours cette option parce que très souvent, si c'est un site qui est détourné on a une victime de plus. Donc il faut en tenir compte dans notre travail.

Aux États-Unis, avoir un accès non autorisé pour un système informatique protégé est une violation.

HILDE THUNEM

Oui, je suis heureuse de voir que vous travaillez avec les noms de domaine détournés, vous avez dit que le plus grand de cas était des cas de hameçonnage et des fraudes. Comment faites-vous pour

contacter une personne et lui dire que son site est détourné ? Je sais qu'en tant qu'opérateur de registre, nous sommes très invisibles, c'est difficile de contacter une personne et de lui dire cela, on va être considéré comme des fraudeurs nous-mêmes, c'est mieux que ce soit a police ou quelqu'un d'autre, quelqu'un qui va dire à ce client, parce que sinon on risque d'avoir des problèmes. En même temps on nous demande de faire quelque chose et rapidement, parce qu'il y a des dommages qui existent. Je parle de fraudes.

GABRIEL ANDREWS

Oui, je suis tout à fait d'accord avec vous, nous sommes dans la même situation, vous avez raison il y a des défis, on ne sait pas comment le dire aux victimes. On a collaboré avec le secteur privé et ces collaborations peuvent comprendre des compagnies importantes, des compagnies de fournisseurs de services internet, et même Microsoft. Ici il faut trouver l'équilibre pour voir dans quelles mesures vous devez le dire à la personne, vous devez prévenir la police. Parfois c'est quelque chose qui est arrivé dans les cas d'empoisonnement du DNS et c'est très compliqué que le fournisseur de services internet annonce à son client cela, parce que le client va commencer à accuser le fournisseur de service et de lui dire qu'il est responsable de la situation. Donc c'est important, en tout cas je parle dans le cadre de notre agence, de notre service, c'est une situation compliquée, on ne sait jamais très

bien comment faire pour annoncer ce type de mauvaise nouvelle au client.

NICK WENBAN-SMITH Pierre et ensuite Bryan. D'abord, Hilda, est-ce que vous soutenez un opérateur de registre ? Est-ce que vous voulez introduire des requêtes juridiques et autres ?

HILDE THUNEM Non. Parce qu'ils achètent un nom de domaine, ils achètent un droit pour être dans une base de données, pour avoir une adresse IP, ils ne sont pas obligés d'avoir un site internet, ils ont choisi d'avoir certains services, c'est un choix. Ils sont responsables selon la loi de communication électronique en Norvège pour l'utilisation du nom de domaine. Donc je mets dans le contrat qu'ils doivent faire certaines choses que je ne fournis pas moi-même. Et je pense que c'est important que cela figure dans le contrat.

Quand on traverse la rue, on doit regarder à droite et à gauche et bien c'est pareil. Lorsque vous achetez ce type de service, vous devez tenir compte de certains délits.

NICK WENBAN-SMITH Pierre ?

PIERRE Merci, Nick et merci pour cette séance très intéressante. D'abord, je souhaitais dire que, comme d'habitude, je suis tout à fait

d'accord avec Hilda, avec .NO, cela ne signifie pas que nous ne devions pas réagir quand nous voyons qu'il y a un problème sur un site internet. Mais c'est une situation différente. Si vous mettez dans un contrat que vous devez garantir que vous allez maintenir la sécurité de votre site internet, la question que je poserais ensuite c'est : comment je peux faire respecter mon propre contrat, comment vérifier que le titulaire a vraiment protégé son site internet ?

Donc je ne peux pas introduire quelque chose dans un contrat que je ne peux pas faire respecter.

La question aux intervenants maintenant, notamment la personne du FBI. Si vous pouvez partager des informations concernant le type de discussions que vous avez avec les compagnies de téléphones, parce que nous parlons des données de WHOIS et, très souvent, les escroqueries dont j'entends parler c'est un SMS que je reçois sur mon téléphone et ce ne sont pas des numéros cachés, donc c'est une escroquerie qui utilise des numéros de téléphone qui existent. Donc ces personnes ne donnent pas leur véritable adresse ou leur véritable nom aux opérateurs de téléphone, sinon ce serait trop facile de les attraper.

Je ne sais pas comment cela fonctionne, mais je pense que nous voyons de plus en plus de fournisseurs d'internet de banque ou de téléphone qui demandent de faire des vérifications que les télécoms devraient faire. Et cela ne marche pas. Donc je voudrais savoir comment gérer cet aspect du problème.

GABRIEL ANDREWS

Je reconnais que c'est une question juste, mais je n'ai pas de réponse à vous donner, je m'en excuse. Je n'ai pas parlé avec les opérateurs de télécommunication dernièrement, cela fait bien longtemps. Et je dirais qu'il y a une reconnaissance croissante selon laquelle il y aurait beaucoup de défis et problèmes concernant l'authentification de l'identification, le fait de savoir l'identification réelle d'une personne. Il y a des outils comme l'IA qui permettent de se faire passer pour une personne. Vous vous rendez compte des défis ? Quand on parle avec une personne, comment être sûrs qu'on parle vraiment avec cette personne ? Donc, comment avoir confiance dans les systèmes actuels ? C'est très compliqué. Il y a beaucoup de choses à dire et je ne suis pas la personne indiquée.

PIERRE

Je comprends bien, mais c'est une manière aussi d'attirer votre attention sur ce point, parce que les numéros sont aussi des identificateurs, personne ne pense qu'un numéro de téléphone est faux. Les noms de domaine aussi sont des identificateurs. Donc il y a des liens réels entre un numéro de téléphone, un nom de domaine et une personne. On devrait pouvoir essayer de savoir comment ils font dans l'industrie des télécommunications parce qu'on parle toujours d'identificateurs, nous.

NICK WENBAN-SMITH Merci. Je vais maintenant donner la parole à Bruce puis à Keith.

BRUCE TONKIN Et bien oui, chaque groupe dit que c'est le problème de l'autre, on s'accuse mutuellement et le nom de domaine, c'est un lien qui est en relation avec un message SMS, par exemple en Australie aussi on a ce type d'escroquerie qui fonctionne par SMS. On peut rapporter l'escroquerie, mais est-ce que cela sert à quelque chose ? On ne sait pas. Il est difficile en tout cas de collecter toutes les données dans ce problème. Les registres ont des numéros de téléphone, voilà, tout cela est difficile à collecter.

KEITH DRAZEK Merci pour cette question. Je voudrais dire que le forum d'infrastructure de l'internet essaye de voir comment tout cela évolue et inclure les télécommunications et le processus de paiement quand on commence à parler de fraudes financières ; par conséquent, je pense que les attentes dans ce domaine, au niveau des bureaux d'enregistrement, des registres, des CDN, il y a des acteurs qui ont différents rôles et il faut essayer d'atténuer ces dommages en essayant de connaitre et d'analyser la capacité technique et la responsabilité de chacun de ces acteurs. C'est un de ces objectifs.

NICK WENBAN-SMITH Merci. Dernière question.

BRIAN CIMBOLIC Merci. Je vais poser une question rapide à Gabe. Le rapport des délits sur internet, est-ce qu'il s'agit seulement de délits liés à internet ou à des plateformes de réseaux sociaux ?

GABRIEL ANDREWS Cela comprend tous les délits liés à l'internet. J'essaye de diviser cela, de fournir des données à l'ICANN pour que cela puisse être analysable et voir dans quelles mesures cela affecte le DNS, mais je dirais que c'est très compliqué.

BRIAN CIMBOLIC Et est-ce que vous savez comment ventiler tout cela et quel est le volume de fraudes sur les réseaux sociaux ?

GABRIEL ANDREWS J'aimerais pouvoir vous répondre, mais je ne peux pas. Il y a des catégories comme le hameçonnage, mais je ne sais pas si on peut faire des catégories genre hameçonnage basé sur le WhatsApp, sur les applications de chat, les SMS, c'est très compliqué. C'est une bonne question, mais je ne crois pas qu'on a encore ce niveau de précision.

BRIAN CIMBOLIC Ce serait intéressant de présenter cela à la communauté du DNS, parce que je pense que ce sont des choses qui vont probablement arriver sur les plateformes de réseaux sociaux.

GABRIEL ANDREWS Je suis d'accord avec vous, ce serait bien d'avoir ce type de précision, peut-être que nous y arriverons.

NICK WENBAN-SMITH Merci, c'est compliqué, fascinant. C'est un des objectifs d'avoir ce type de séances, parler des acteurs, des différentes perspectives qui existent, des contextes, essayer de comprendre ces contextes, ces chiffres. C'est très important pour voir ce qu'on peut faire, connaitre les infrastructures et essayer de prévenir ce type de délits et parler avec tous les acteurs impliqués dans ce domaine et comprendre le contexte. C'est important parce qu'il y a beaucoup de plateformes qui sont impliquées ici. Donc une discussion très intéressante.

Donc nous allons passer à notre sondage et j'attends la question, s'il vous plait. Pouvez-vous l'afficher ?

C'est la fin de notre séance, nous voyons qu'il y a un petit changement, mais il y a encore des situations où les registres ne sont pas suffisamment préparés à détecter les utilisations malveillantes du DNS.

Donc je voudrais simplement que l'on puisse applaudir nos panélistes, qui ont fait un travail formidable. Il y a des ressources

qui vous sont proposées dans la bibliothèque et, maintenant, je vais simplement vous permettre de profiter de la pause-café.

[FIN DE TRANSCRIPTION]