ICANN82 | Forum de politiques – Réunion conjointe : GAC et SSAC
Dimanche 9 mars 2025 – 16h30 à 17h30 PST

NICOLAS CABALLERO: Mesdames et messieurs, bienvenue. Nous allons reprendre. Veuillez prendre place dans la salle, s'il vous plaît. Allez-y pour l'enregistrement.

GULTEN TEPE: L'enregistrement a commencé. Bonjour. Bienvenue à la réunion conjointe GAC-SSAC de l'ICANN82, aujourd'hui dimanche 9 mars, 16 h 30, heure locale.

Cette réunion est enregistrée et régie par les normes de comportement attendues à l'ICANN et la politique anti-harcèlement de la communauté de l'ICANN.

Pendant cette séance, les commentaires et questions soumis sur le tchat seront lus à haute voix s'ils sont soumis dans le bon format. Veuillez indiquer votre nom ainsi que la langue dans laquelle vous allez parler, si vous parlez une autre langue que l'anglais. Veuillez parler distinctement et lentement pour permettre une bonne interprétation de vos propos, et assurez-vous de mettre en sourdine tous vos autres dispositifs lorsque vous interviendrez. Vous pouvez avoir accès aux fonctionnalités pour cette séance dans la barre d'outils de Zoom.

Sur ce, je vais laisser la parole à Nicolas Caballero, président du GAC. Merci.

NICOLAS CABALLERO Merci et bienvenue à tous à la dernière séance, mais la plus importante à mes yeux avec le SSAC, Comité consultatif sur la sécurité et la stabilité. Bienvenue Ram ! Bienvenue à votre équipe fantastique !

Et d'ailleurs, on parlait de certaines des questions dont on allait parler aujourd'hui, hier et avant-hier. Et lorsque j'ai parlé d'informatique quantique et de ses effets potentiels sur le DNS et la stabilité du DNS et la mise en œuvre du déploiement du DNSSEC et du chiffrement en général symétrique, asymétrique, etc., et tout le monde me regardait comme si j'étais un peu fou. Ça peut être le cas d'ailleurs. Mais bref, on va parler de tout cela en profondeur avec cette équipe d'éminents experts.

On va parler d'informatique quantique et de son impact sur le chiffrement, comme je l'ai dit hier. Ensuite, on aura une discussion sur INFERMAL. Et pour les seize nouveaux membres du GAC, je vais expliquer de nouveau ce que veut dire INFERMAL — Étude donc d'analyse inférentielle des domaines enregistrés à des fins malveillantes.

Voilà, je vous cède la parole sans plus attendre.

RAM MOHAN

Merci beaucoup et au nom du SSAC, je tiens à vous remercier vivement, vous, les membres du GAC, de cette invitation. C'est la troisième fois que nous nous réunissons avec vous. Et à chaque fois, l'interaction devient de plus en plus riche et beaucoup plus dynamique entre nous. Donc, nous apprécions énormément cette opportunité pour renforcer notre dialogue de coopération sur les questions critiques au niveau de la stabilité et la sécurité de l'Internet.

Pour ceux d'entre vous qui sont nouveaux au GAC et nouveaux dans la communauté de l'ICANN, sachez que le SSAC est l'organe consultatif expert de l'ICANN qui veille à identifier et analyser les menaces potentielles par rapport au système de nommage et d'adressage de l'Internet.

Le SSAC est constitué de techniciens professionnels qui fournissent des recommandations étayées par des preuves au Conseil d'administration et à la communauté de l'ICANN. Parfois, nous ne fournissons pas des recommandations étayées par des preuves, mais des cas. Et nous couvrons toute une série de thématiques : vulnérabilités du DNS, risques par rapport à l'impact des nouvelles technologies sur l'infrastructure de l'Internet, la sécurité et la stabilité et la résilience des aspects liés à la gouvernance de l'Internet. Donc, nous couvrons toutes ces thématiques, mais notre principale mission a à voir avec l'infrastructure critique du système.

Nous comprenons que le rôle fondamental du GAC pour représenter le point de vue des gouvernements sur la gouvernance de l'Internet, parmi d'autres questions, et cette interaction entre nous nous permet à nous, au SSAC, de réunir les aspects techniques et politiques. Et on veut s'assurer que nos recommandations soient à la fois solides et alignées sur l'intérêt public. Ça, c'est l'approche principale qui est la nôtre. Et nous souhaitons partager avec vous nos opinions, écouter votre point de vue pour, ensemble, contribuer à un Internet sûr, stable et intègre.

Donc voilà un petit peu ce que nous faisons et c'est pourquoi cette interaction avec le GAC est si importante pour nous. Nous vous en remercions.

Et comme cela a déjà été dit, nous avons deux thématiques principales que nous aimerions aborder avec vous. Et Russ est ici, à ma droite. Il a une longue carrière dans le domaine, entre autres, de l'informatique quantique, son impact sur le chiffrement. Donc, il m'a semblé important d'inviter Russ pour vous faire part de son expérience dans ce domaine. Notre intention n'est pas de vous faire un masterclass ou de vous assommer d'informations, mais de vous dire un petit peu où on en est, et surtout d'engager une conversation avec vous. On essaie, dans la mesure du possible, de faire en sorte que nos présentations ne soient pas hautement techniques, même si le matériel qui sous-tend ces présentations l'est. Donc c'est là, notre objectif. Si on s'adressait à un public

technique, j'utiliserai des termes beaucoup plus techniques, mais, ici, ça n'est pas le but de l'opération.

RUSS HOUSLEY

Merci Ram. Alors je vous ai indiqué ici un titre sur cette diapo : « L'informatique quantique ». Ça fait un moment qu'on en parle. Et l'Institut ISO a beaucoup réfléchi à la question. Et la solution s'appelle ML-DSA. C'est-à-dire norme de signature numérique basée sur un réseau de treillis. Et la solution ne s'intègre pas parfaitement bien au DNSSEC. Il s'agit d'avoir des signatures très grandes. Si vous utilisez DNS sur UDP, ça ne fonctionne pas.

Donc la bonne nouvelle, c'est que nous avons eu pas mal de temps pour y réfléchir, parce que la grande préoccupation par rapport à l'informatique quantique, c'est ce qu'on appelle l'attaque.

Et si vous avez toute une série de secrets, et l'attaque les enregistre et les stocke jusqu'à ce qu'ils aient une informatique quantique qui lui permette de révéler ces secrets, obtenir les clés et déchiffrer les secrets — dans le DNS, il n'y a pas de secret. Donc ce n'est pas un problème. Ce qui nous préoccupe ici, c'est que nous avons une signature numérique qui ne peut pas être copiée. Avant qu'on puisse réellement atténuer l'existence de l'informatique quantique. Donc il faut essayer d'appliquer ces signatures numériques.

Donc voilà la recherche qui est en cours. L'IETF a un groupe qui se penche sur le DNSSEC post-quantique, et va se réunir la semaine

prochaine. Et la réponse au blockchain, à la transparence des certificats et de toute une série d'autres technologies, ça semble être le Merkle.

Ici, je vous ai indiqué des liens. Lorsqu'on parle de signature, ce qui s'applique ici, c'est que ces signatures sont également très vastes. Donc il faut trouver d'autres techniques. Bref, il va y avoir énormément de discussions à l'IETF la semaine prochaine pour explorer tout cela. Mais je ne m'attends pas à ce qu'on ait une réponse avant un an. Mais bon, on a le temps.

Donc si vous avez des questions là-dessus ? Ou est-ce qu'on les prend à la fin ? D'accord. Bah écoutez, si vous avez des questions, je serai ravi d'y répondre.

NICOLAS CABALLERO Merci beaucoup ! Vous avez la possibilité de poser des questions maintenant. Alors est-ce que vous pourriez expliquer ce que veut dire signature numérique ? Qu'est-ce que ça veut dire en termes très simples ?

RUSS HOUSLEY Oui, alors signature numérique, c'est ce que le DNSSEC fait. L'idée, c'est que lorsque vous obtenez la réponse à votre demande, la signature numérique y est jointe. Ça veut dire qu'elle n'a pas été modifiée depuis qu'elle a été publiée à l'origine. Donc c'est ce qui donne la garantie de l'authentification et de l'intégrité des données elles-mêmes.

NICOLAS CABALLERO Merci beaucoup. J'ai les Pays-Bas qui souhaitent intervenir.

MARCO HOGEWONING Représentant des Pays-Bas, Marco Hogewoning au micro.

Oui, je suis d'accord avec vous. Il y a encore beaucoup de chemin à parcourir. Toutefois, je représente mon gouvernement. Et je sais que parfois on pense que les choses vont arriver dans longtemps, et elles arrivent tout de suite.

Donc, sans rentrer dans trop de détails techniques, est-ce qu'il y a un conseil concret que vous pourriez nous donner à nous les gouvernements, dès maintenant, et que pouvons-nous faire pour nous préparer à ce qui sera l'issue inévitable, c'est-à-dire changer l'algorithme du DNSSEC ?

RUSS HOUSLEY Il y a d'autres protocoles pour lesquels on a des solutions. On a travaillé au sein d'autres groupes de travail de l'IETF, comme LAMPS qui travaille sur les paquets, et même on a TLS et IPSEC. Et dans ces trois domaines -- et Secure Shell aussi. Et dans ces quatre domaines, nous avons des solutions où l'infrastructure va être déployée maintenant -- est censée être déployée maintenant. Donc si on en a besoin maintenant, elle peut être déployée.

Maintenant, la transition de SHA-1 à SHA-256, moi, j'ai été chef de la sécurité à l'IETF à l'époque, et je pensais que ça allait prendre

cinq ans. Et ça a pris le double. Donc, la transition peut se produire parce qu'il y a toute une série de choses par la suite qui ne peuvent pas se produire s'il n'y a pas l'infrastructure nécessaire en place. Donc ça, c'est l'avis que je pourrais vous donner.

NICOLAS CABALLERO Steve.

STEVE CROCKER Oui, alors j'aimerais rebondir sur cette question parce que, effectivement, les gouvernements peuvent se demander ce qu'ils peuvent faire.

Alors, on a un certain nombre de problèmes qui se posent par rapport à SHA-256. Alors, à quoi ressemblerait cette transition si, au moment où il y a une décision qui est prise par rapport à ce nouvel algorithme, si on passe à ce nouvel algorithme. Est-ce que ce sera différent d'un point de vue quantitatif par rapport aux transitions qu'on va avoir ? Ou bien est-ce que ce sera un changement d'algorithmes pour lequel on n'a pas encore d'expérience ni de pratique ?

RUSS HOUSLEY Merci, Steve Crocker. Alors, on n'en est pas certains. Ça, c'est la réponse la plus simple.

Ce que l'on sait, c'est que celui-ci est plus compliqué parce qu'il ne s'agit pas simplement de changer l'une des pièces du changement

de vitesse. Il s'agit de changer toute la boîte de vitesses. Donc on est dans une situation où, si on pense à un PKI, il faudrait penser à créer un nouveau PKI depuis la racine jusqu'à la fin, et non pas une seule pièce.

J'espère avoir ainsi répondu à votre question. Non, ce n'était pas utile, ma réponse ? D'accord.

NICOLAS CABALLERO Merci, Steve Crocker, de cette question. Et merci, Russ, de la réponse. Y a-t-il d'autres questions ou commentaires ? J'ai une question.

Imaginons qu'un gouvernement X a un très bon déploiement du DNSSEC, MANRS et RPKI, etc. Toute combinaison de Blowfish, RSA… Bref, quelle qu'en soit la combinaison. Et tout d'un coup, il y a une avancée extraordinaire d'informatique quantique. Alors, dans ce cas-là, au niveau de la structure du DNSSEC, toute l'infrastructure du gouvernement serait totalement obsolète. C'est bien ça ?

RUSS HOUSLEY Oui, mais on ne sait pas exactement quand. Il y a beaucoup d'écrits, actuellement, qui traitent des avancées en matière du nombre de qubits et de la taille des ordinateurs quantiques. Mais pour l'instant, on n'est pas proche d'arriver à un point de bascule pour ce qui est du chiffrement. Et tout cela n'est pas linéaire. Les percées peuvent se produire soudainement et être considérables, mais ce

n'est pas prévisible. Donc on n'aura forcément pas d'avertissement. Donc c'est pour ça qu'il faut commencer à plancher sur cette question maintenant.

Mais pour ce qui est des PKI du DNSSEC, ils sont uniques, car ils ont simplement besoin d'intégrité. Il n'y a pas de problèmes liés à la récupération de secret. Donc on a plus de temps, parce qu'il n'y a pas de problème de protection des secrets. Donc si on combine bien MANRS, RPKI et DNSSEC, ça devrait aller. On a un peu plus de temps pour gérer ces questions, car on ne gère que des données publiques et on ne gère que l'intégrité de l'architecture pour ces données publiques.

NICOLAS CABALLERO Donc j'ai d'abord l'Australie, puis les Pays-Bas.

INGRAM NIBLOCK Je sais qu'il y a différents objectifs pour ce qui est du DNS HTTPS ou DNS TLS. Il y en a un qui signe et un qui transporte. Mais est-ce que l'on pourra facilement mettre en œuvre les nouveaux algorithmes de chiffrement post-quantiques pour ce qui est de ces éléments-là ? Est-ce que l'on va pouvoir convertir les avantages du DNSSEC, notamment pour ce qui est du transport de certaines informations ?

RUSS HOUSLEY Oui et non. Oui, l'on pourra protéger le trafic entre le point de chiffrement et le point de déchiffrement. C'est un système qui va

d'un point A à un point quand on l'applique au DNS. Cela fournira de la protection dans ce cadre. Évidemment, le TLS est en cours et on n'a pas encore le PKI auquel il peut s'accoler. Et par ailleurs, le formulaire, c'est un browser. On a une réunion après la réunion du Groupe de travail sur le génie de l'Internet à Tokyo.

NICOLAS CABALLERO

Donc merci à l'Australie. Alors pour les nouveaux membres GAC, PKI, c'est Infrastructure publique clé, et MANRS, eh bien, ce sont les infrastructures militaires.

Donc les Pays-Bas.

MARCO WOGEWONING

Alors je fais un pas de côté. Je ne veux pas me faire l'avocat du diable, mais je ne veux pas que l'on parle trop de technique.

Alors, sur la planche précédente, tu parles des difficultés en matière de transport UDP. Ce n'est pas la première fois que, dans le champ du DNS, on a des limites avec le transport UDP. Mais je pense que c'est aussi un problème pour le DNS, la mise en œuvre du DNSSEC pour ce qui est de la longueur des clés. Lorsque l'on se penche sur le long terme, eh bien, peut-on envisager d'avoir différentes options de transport autre que le DNS pour l'UDP ?

RUSS HOUSLEY

D'autres options de transport ? Oui, elles sont bien comprises et bien spécifiées, mais elles ne sont pas bien déployées. Donc voilà.

MARCO WOGEWONING Oui, nous sommes du gouvernement. Alors, comment pouvons-nous vous aider ?

NICOLAS CABALLERO Russ, peux-tu nous donner quelques exemples à propos de l'UDP ?

RUSS HOUSLEY Pour ce qui est de DNS sur TCP ou DNS sur QUIC ou DNS sur TLS, ce sont des exemples d'éléments qui n'ont pas le même nombre de limitations par message.

PETER THOMASSEN J'ai l'impression que certains des éléments évoqués peuvent être dits de façon moins technique. Russ a dit un peu plus tôt que les signatures étaient attachées aux réponses DNS et que ces signatures attestent du fait que l'information DNS n'a pas été changée depuis qu'elle a été publiée.

Bon, si chacun pouvait attacher une signature, ce ne serait pas très utile. Pour attacher une signature, il faut avoir le contrôle d'une clé privée et il faut cela pour pouvoir calculer la signature. Donc, la menace que font peser les ordinateurs quantiques, c'est l'extraction de cette clé, même si vous n'avez pas le droit de l'avoir. Et ensuite, vous pourriez créer de fausses signatures.

Une autre application de la cryptographie, c'est le chiffrement, c'est-à-dire la protection de données secrètes que vous pouvez

rendre illisibles, à moins de posséder la clé de déchiffrement. Donc, encore une fois, on utilise des clés.

Et il est important de reconnaître que l'informatique quantique fait peser une menace sur ces deux applications, le calcul des signatures, les clés secrètes ou les clés de chiffrement de déchiffrement. Mais ce sont deux cas d'application différents et le DNS ne s'applique pas au chiffrement-déchiffrement. Le DNS permet de contrôler, à un moment donné. Lorsqu'on cherche à se connecter quelque part et que l'on fait une requête DNS, on peut calculer la validité de la signature.

Donc si vous voulez changer cela avec un ordinateur quantique, il faudra faire cela très rapidement, quasiment en temps réel. Alors que si vous avez enregistré des informations chiffrées venant d'un transfert HTTPS par le passé, eh bien, vous pouvez prendre cinq ans pour déchiffrer cela. Donc, si vous avez un ordinateur quantique qui est efficace, mais lent, eh bien, cela va faire peser une menace sur vos données chiffrées, mais cela ne va pas faire peser de menace sur vos informations DNS, car si cela prend cinq ans pour forger une signature, eh bien, personne n'est plus intéressé par cette information, car la connexion se fait en quelques secondes.

Alors, conclusion ? Que peuvent faire les gouvernements ? C'est-ce que les Pays-Bas ont demandé à propos du DNS. Ne paniquez pas. C'est un problème qui relève de la recherche scientifique pour l'instant. Il faut suivre cela de près, si vous êtes intéressés. Mais je

pense que le problème le plus immédiat, c'est plutôt la protection des données stockées ou en transit — données que l'on veut garder secrètes. Il y a les mêmes problèmes d'extraction, mais c'est beaucoup plus urgent, et il y a beaucoup plus de progrès en la matière qu'il y en a dans le champ du DNS.

NICOLAS CABALLERO Merci.

RUSS HOUSLEY Merci de présider la séance la semaine prochaine.

RAM MOHAN Merci Nico. Ce que j'aimerais proposer aux GAC, peut-être que l'on peut avoir une petite présentation sur ce champ, avec quelques supports qui pourraient vous aider ou qui pourraient aider vos membres en tout cas, lorsqu'ils collaborent dans ce champ. Je pense qu'il faut vraiment comprendre cette distinction. Il faut faire passer le message auprès des autres acteurs de votre gouvernement.

Donc il faut bien comprendre ce qu'est le désavantage de l'informatique quantique sur la sécurité du DNS et le désavantage d'avoir l'informatique quantique pour la protection des données secrètes.

NICOLAS CABALLERO

Merci Ram. Merci Russ. Alors cinq ans, je ne sais pas. Peter, je ne comprends pas trop. En tout cas, merci de cette explication. J'espère -- enfin j'espère, je n'espère pas, mais je pense qu'il y aura des surprises dans un avenir proche.

Avant que je donne la parole à Jeff, avez-vous des questions à poser en salle ou en ligne ?

Merci Russ. Je donne la parole à Jeff. Jeff, tu as la parole.

JEFF BEDSER

Merci Nico. Jeff Bedser pour le SSAC. Donc on a évoqué la possibilité de parler de cette étude INFERMAL, analyse inférationnelle des noms de domaine enregistrés à des fins malveillantes. Donc c'était soumis par l'OCTO. Il y a une composante de recherche scientifique. Et donc cette unité s'est penchée sur des enregistrements à des fins malveillantes, utilisés notamment pour de l'hameçonnage.

Donc, l'un des premiers éléments que je veux évoquer, c'est que ce n'est pas un rapport qui propose des solutions, mais c'est un rapport qui est conçu pour répondre à des questions qui ont été posées par la communauté, et ce, depuis un moment, à propos de l'influence de certains facteurs, et notamment la façon dont les cybercriminels obtiennent des noms de domaine à des fins malveillantes.

Donc le rapport fournit des informations quant aux incentives économiques, la vérification proactive, les restrictions importantes

pour ce qui est d'atténuer les utilisations malveillantes des noms de domaine. Il propose également des stratégies pour lutter contre les abus.

Alors voici quelques-uns des constats, si vous n'avez pas lu le rapport. Donc il y a les incitatifs économiques. S'il y a des frais d'enregistrement plus faibles, eh bien, chaque dollar en moins pour les frais d'enregistrement correspond à une augmentation de 49 % de noms de domaine malveillants. Et les services gratuits, s'il y a la disponibilité de services gratuits, tels que l'hébergement Web, eh bien, il y a 88 % d'augmentation des activités d'hameçonnage pour les réductions. Les réductions sur les enregistrements de nom de domaine sont associées à des augmentations considérables d'enregistrement malveillantes. S'il y a des mesures proactives à mettre en place, il y a des restrictions qui sont strictes, eh bien, on peut réduire les abus de 63 %. Accès API, s'il y a une API qui est fournie par les bureaux d'enregistrement, eh bien, et s'il y avait des pratiques de vérification, il—

Bon, pour ce qui est des mesures réactives. Temps d'atténuation. L'incidence des temps d'atténuation sur les domaines de réduction est minimale. Pour les bureaux d'enregistrement, les préférences TLD, donc la concentration des abus. Les enregistrements malveillants ne sont pas distribués de façon uniforme et semblent se concentrer sur certains bureaux d'enregistrement et TLD.

Et puis, il y a les pratiques des bureaux d'enregistrement. Si les bureaux d'enregistrement offrent des prix plus faibles et des services -- plus des services gratuits, ils sont plus à même d'attirer les utilisateurs et enregistrements malveillants.

Ce sont des informations qui ont été bien comprises par la communauté anti-abus depuis un moment. Ce qui importe, c'est la question économique. Les acheteurs se tournent vers le prix le plus faible, là où ils peuvent acheter en gros. Dans la plupart des pays du monde, il y a des entités qui vendent en gros pour toute une série de produits et de biens. Ils le vendent au prix le plus faible.

Alors on peut analyser les données ainsi, mais cela ne signifie pas que l'on va résoudre le problème. Car si l'on fait augmenter le prix, eh bien, vous avez toujours un prix plus faible quelque part, à moins de s'entendre au niveau du prix sur toute la planète. Et au vu de toutes les économies différentes, de toutes les devises différentes, cela va être problématique et vous n'allez pas pouvoir éliminer le problème.

En outre, les pertes en matière de cybercriminalité, eh bien, divergent. Il y a des estimations qui vont de 1000 milliards à 10 000 milliards. Et donc c'est une différence considérable. Alors, par victime, on estime qu'il y a une perte de 136 USD. Mais aux États-Unis, cette perte par victime d'hameçonnage s'élève à 3 520 USD. Donc, j'ai vu toute une série de chiffres différents. Et je suis certain que ceux qui travaillent dans ce champ ont déjà vu ces chiffres. Mais la réalité est que si chaque perte minimale représente

136 USD, eh bien, il faut se demander ce que l'on doit facturer pour un nom de domaine. Car de toute façon, il faudrait fixer le prix du nom de domaine à un montant très élevé si l'on voulait éviter cela.

Donc il faut réfléchir à ce que peuvent faire les politiques pour réduire les utilisations malveillantes en matière de cybercriminalité, en matière d'hameçonnage. Et il faut se demander si changer le prix va permettre de modifier les comportements des criminels. S'ils peuvent générer des centaines de milliers de dollars, est-ce que l'on va pouvoir le faire si le nom de domaine passe de 2 USD à 10 USD par an ?

Prochaine planche.

Processus de vérification. Comme je l'ai dit, l'étude a été publiée en novembre. Et donc c'est fondé sur les données disponibles à l'époque. Et les questions liées à l'intelligence artificielle continuent à s'accélérer à un rythme qui est supérieur à celui du développement de l'informatique quantique.

Mais la possibilité est maintenant de créer des identités numériques générées par l'IA. Dire à un algorithme : J'ai besoin d'un permis de conduire de ce pays avec le nom d'une personne réelle qui y vit et avec une photo qui ressemble à mon visage, ou mettez ma photo pour pouvoir générer de manière numérique une identité qui vous permet d'enregistrer un nom de domaine. Ça, c'est réellement ce qui va avoir un impact sur ce qu'on fait. Parce que si on doit vérifier l'identité de chaque titulaire d'un nom de domaine, on peut régler ce problème. Mais lorsqu'il s'agit d'une

personne réelle avec une photo fausse, imaginez, il va falloir utiliser l'IA pour lutter contre cela. Parce qu'on n'a pas les moyens humains de lutter contre cela.

Donc, quel meilleur processus utiliser pour éviter et aider à lutter contre ces domaines qui sont enregistrés de manière frauduleuse ?

Il y a également la question du taux de détection pour la délégation. Et ce que je suggère ici, c'est que la plupart des études qui ont été réalisées utilisent des sources qui sont disponibles au grand public. Alors, ne vous méprenez pas, les chiffres sont alarmants dans ces études. Mais ce que je veux dire, c'est que le plus gros problème vis-à-vis des utilisations malveillantes du DNS est l'hameçonnage. C'est qu'il faut que les entités les voient et déclarent ces incidents.

Donc ce qu'on voit dans les rapports, c'est des rapports qui font état de dommages. Combien d'entre vous ont reçu un spam et vous l'avez supprimé. Alors, si vous avez notifié cet incident, très bien. Je vous félicite. Mais ça n'est pas le cas de la plupart des gens. Donc, il y a un volume énorme de ce genre de dommage qui n'est pas notifié. Donc modifier la méthodologie pour enregistrer, ça peut-être une solution potentielle ou une voie à suivre. Mais également avoir de meilleures opportunités pour détecter, pour mieux atténuer. Et qu'en six ou sept secondes, on puisse anéantir la menace. Tandis que s'il faut notifier, modifier, ça prend plusieurs jours pour déposer la plainte. Alors que si on pouvait faire une

meilleure détection, on pourrait anéantir immédiatement la menace.

Et il y a également la question des mesures. C'est très difficile de mesurer ce genre de choses. On devrait le faire déjà. Mais le nombre de victimes par domaine, parce que vous pouvez avoir une centaine de victimes par seconde pour un hameçonnage bien fait, donc il s'agit de voir le nombre de victimes qui tombent aussi pour pouvoir mesurer l'ampleur du problème. Parce qu'on sait que même si la pointe de l'iceberg, ce sont les sources disponibles au grand public, avec des hameçonnages et des milliers de domaines qui sont utilisés, on sait qu'il y a énormément de menaces qui ne sont pas notifiées. Mais on ne sait pas non plus le nombre exact de victimes qui sont touchées.

Donc voilà, je vous indique cela comme point de discussion pour l'avenir. Parce que si on a un bon processus de vérification, un bon processus de validation, oui, on sait qu'avec une mauvaise validation et vérification, alors, on a un problème au niveau du trafic.

Et là, je vois qu'il y a un écho qui a été ajouté à ma voix.

Alors, comment faire en sorte qu'on puisse mieux analyser et évaluer l'impact, et comment mieux détecter pour qu'on puisse être plus efficaces pour régler ce problème ? Parce que je pense que même si on facture 1 000 USD par domaine par année, alors on empêche la plupart des gens sur la planète de pouvoir enregistrer un nom de domaine parce que ça va impliquer 20 000 USD par

domaine pour les coûts engendrés. Donc, il faut trouver d'autres solutions. Voilà. Merci.

NICOLAS CABALLERO Merci Jeff. Oui. Est-ce qu'on peut passer à la diapo suivante ? Oui.

Alors, l'augmentation de 400 %, j'aimerais qu'on aborde cette discussion maintenant. Et ensuite, tout ce qui concerne l'API, interface de programmation d'application, qu'est-ce que vous en pensez ? Est-ce que c'est réellement ça, le problème — que les mauvais acteurs aient accès à l'API et qu'ils utilisent l'intelligence artificielle ou autre ? Et ils sont ainsi plus à même d'engendrer des dégâts et d'avoir des activités illicites ?

JEFF BEDSER Oui, je n'ai pas l'ombre d'un doute du fait que les enregistrements groupés soient le moyen de réaliser ces activités. Alors un mauvais acteur qui enregistre des domaines pour un réseau zombie ou pour une campagne de logiciels malveillants peut enregistrer plus d'un millier de noms de domaine et le pourcentage par rapport à l'API, c'est celui-là.

Et d'un autre côté, est-ce qu'il faudrait qu'il y ait des freins ? C'est-à-dire que si une personne enregistre 50 domaines, on pourrait vérifier est-ce que ces domaines vont être enregistrés à des fins malveillantes ou pas. Mais enregistrer 10 000 domaines en même temps, je pense que cela ne devrait pas être permis. Mais l'API en

soi, ça n'est pas le problème. C'est de bien comprendre dans quelles fins sont enregistrés les noms de domaine.

NICOLAS CABALLERO

Merci Jeff. Alors, voyons s'il y a des commentaires ou questions de la part des membres du GAC dans la salle ou en ligne. Vous avez la parole.

Je ne vois pas de main levée. Ah ! Excusez-moi. Si, il y a deux mains. L'inde et l'Australie. L'inde, je vous en prie. Merci.

SUSHIL PAL

Merci, Monsieur le Président. Représentants de l'Inde au micro. Il est clair que la vérification, c'est un problème.

Je pense que si on a les identifiants vérifiés des bureaux d'enregistrement, alors la probabilité d'une utilisation malveillante du DNS s'en voit réduite. Et ça s'est reflété dans l'utilisation des algorithmes. Ce n'est pas l'API le problème ni l'intelligence artificielle. Mais ce sont les identifiants non vérifiés. Donc le problème est très clair.

Il n'en demeure pas moins qu'on ne sait pas comment définir l'exactitude des données. Ça, on le voit au niveau de la GNSO, la portée des données. Et sans aborder à fond cette question de l'exactitude des données acquises, on ne peut pas traiter la question liée à la vérification. Donc, est-ce que, vous, vous pouvez faire pression sur la GNSO pour accélérer les choses à ce niveau-là ?

Parce que, finalement, on sait quel est le problème, mais aucune mesure concrète n'est prise pour régler le problème.

JEFF BEDSER

Alors ce que je n'ai pas dit pendant ma présentation et j'aurais dû être très clair à ce niveau-là, c'est que les gens qui utilisent les noms de domaine à ces fins-là ont énormément de longueur d'avance par rapport à nous. Et la tendance récente a voulu que les personnes légitimes avec des identifiants légitimes vont créer un compte. Et petit à petit, en quelques mois, ils ont un portefeuille de domaine qu'ils vendent ensuite à des mauvais acteurs. Donc même s'il y a une meilleure vérification, c'est très certainement une bonne chose.

Mais trouver une solution, c'est ça, le problème. Et l'autre grande préoccupation, c'est que c'est une séance publique. Et je peux vous assurer que ceux contre lesquels on se bat vont regarder le rapport de cette réunion, et ils vont regarder ce qu'on sait sur eux et ils agiront en conséquence. Donc, je pense que cette question de ce qui nous attend pour la suite, ça nous renvoie à ce que je vous disais dans la présentation. On a besoin d'une meilleure détection. Et avec une meilleure détection, on va pouvoir accélérer le processus d'atténuation. Parce qu'on ne peut pas retirer tout ce qui est encouragement économique, mais si on peut trouver le moyen de détecter pour atténuer, alors les encouragements économiques disparaissent.

Je ne sais pas si je devrais dire ça, d'ailleurs, aujourd'hui, mais on a besoin de meilleure détection et meilleure atténuation.

SUSHIL PAL

Alors lorsque je dis vérification, je pense que c'est une première étape. On parle, on parle, mais on ne prend aucune mesure concrète, en particulier du côté des gTLD. On n'a pas de problème au niveau des ccTLD.

Je peux parler de l'expérience de mon pays où on a mis en place un processus à deux facteurs, et les chiffres ont été énormément réduits. Cela représente un coût pour les bureaux d'enregistrement et c'est un coût énorme qu'on paye tous. Et il est important pour nous de reconnaître qu'il faut prendre une première mesure sans pour autant sous-estimer l'importance de la détection.

NICOLAS CABALLERO

Merci beaucoup l'Inde. J'ai l'Australie, la Commission européenne, le Royaume-Uni et les Pays-Bas.

INGRAM NIBLOCK

Par rapport aux prochaines étapes dans l'étude INFERMAL, bien entendu, il y a des conclusions -- il ne s'agit pas de conclusions ni de solutions qui sont données dans ce rapport. Mais est-ce qu'il y a un moyen de valider cette hypothèse avec les bureaux d'enregistrement ? Parce que vous avez des domaines particuliers qui figurent sur la liste de noms de domaines bloqués. Alors qu'est-ce que les gens qui ont fait une utilisation malveillante du DNS ont

fait avec les données dont disposaient les bureaux d'enregistrement ? Donc voilà, je me demandais quelles étaient les prochaines étapes pour la recherche.

JEFF BEDSER Alors là, je dois vous renvoyer au bureau du CTO pour répondre à cette question. Ce sont les auteurs de ce rapport. Et les prochaines étapes, je ne sais pas. Voilà ce que je peux vous dire pour l'instant.

NICOLAS CABALLERO Merci l'Australie. La Commission européenne.

GEMMA CAROLILLO Gemma Carolillo, la Commission européenne.

Ma collègue en a déjà parlé sur le tchat. Nous allons avoir une présentation lors de la séance sur l'utilisation malveillante du DNS. Et OCTO va également intervenir. Donc je leur poserai certaines de ces questions. Mais j'ai une question.

D'abord, une question générale. Étant donné que les répercussions de cette étude ou ce rapport INFERMAL, est-ce que vous avez des commentaires sur ce rapport ? Est-ce que vous avez une liste de commentaires sur ce rapport auxquels on pourrait avoir accès ? Parce que ça, ça nous aiderait aussi à examiner et lire ce document.

Ensuite, je comprends que l'API n'est pas un problème en soi. Mais étant donné que les enregistrements groupés semblent être le problème, alors quelle est la conclusion qu'on peut en tirer ? Est-ce

qu'il faudrait établir une restriction par rapport à l'utilisation de l'API ? Est-ce qu'il faut adopter une certaine pratique par rapport à l'enregistrement groupé ?

JEFF BEDSER

Pour répondre à la première question, alors ces éléments de langage ne proviennent pas d'un document de consensus du SSAC. Nous pouvons évidemment reprendre ça au niveau des chefs de file, pour savoir si l'on peut avoir un consensus quant à l'interprétation d'INFERMAL et voir si on peut faire émerger un consensus. Mais oui, on pourra organiser un suivi là-dessus.

Et j'ai oublié la deuxième question, désolé. Les pratiques vis-à-vis de l'enregistrement groupé. Alors pour ma part, moi, j'envisage des occasions. Imaginez une entreprise qui veut créer une nouvelle identité de marque et qui veut enregistrer cette identité sur toute une série de noms de domaine de premier niveau. Il peut s'agir de 2000 enregistrements à ce stade. Et dans ce cas-là, ces outils pourraient être justifiés. Mais je ne vois pas quelle justification à un enregistrement groupé de plus de 2000 éléments. Peut-être que je n'ai pas suffisamment d'imagination.

Mais pour répondre à l'Inde, rebondir sur ce qu'a dit l'Inde, avant, il faut des règles pour avoir un permis moto. Il y a des règles différentes pour un permis voiture et pour un permis poids lourd. Donc vous avez des conditions plus ou moins strictes en fonction du danger que représente le véhicule.

Et si l'on doit faire une comparaison, eh bien, je dirai que l'API, eh bien, c'est l'équivalent du poids lourd. Il faudrait avoir des conditions bien plus strictes pour y accéder. Bon, évidemment, ce n'est pas un problème qui relève de l'outil lui-même, mais plutôt de qui a la possibilité d'utiliser l'outil.

NICOLAS CABALLERO Merci. Le Royaume-Uni.

NIGEL HICKSON Nigel au micro, pour le Royaume-Uni.

Tout cela est très intéressant. Cela nous permet de contextualiser le rapport. Et merci au SSAC de s'être penché dessus. Bon, je sais que l'on en est aux balbutiements seulement, et je me demande si cela pourrait éventuellement prendre la forme d'une recommandation. En tout cas, au vu du poids qu'ont vos recommandations, eh bien, cela pourrait avoir du sens ici.

RAM MOHAN Merci Nigel. On n'en est pas encore à ce stade. On n'est pas encore prêt à formuler une recommandation à ce propos. On va présenter des éléments au SSAC aussi -- OCTO doit présenter des éléments au SSAC. Mais ce que l'on n'a pas encore fait, c'est constater s'il y avait des éléments supplémentaires à prendre en compte.

Je pense en effet qu'il y a peut-être d'autres travaux qui doivent prendre place et qui relèvent plutôt de l'élaboration des politiques

plutôt que de relever du conseil technique. Le rapport INFERMAL a fourni pas mal de conseils techniques. Ce sont mes réflexions. Mais au SSAC, on n'a pas encore évoqué cela précisément. Mais en tout cas, merci de cette suggestion.

On va assurément en parler lorsqu'on parlera de ça au sein du SSAC, pour savoir ce qu'en pensent les membres.

NICOLAS CABALLERO Merci Ram. Les Pays-Bas.

MARCO WOGEWONING Marco au micro, pour les Pays-Bas.

Pour ce qui est de l'atténuation, eh bien, oui, c'est vraiment un problème qui relève des politiques. Mais l'on doit pouvoir également améliorer la détection et l'utilisation des API. Et je pense que cela doit faire lieu d'un débat hors du champ politique. Peut-il y avoir des normes techniques qui peuvent améliorer la détection ou l'utilisation des API pour nous aider à résoudre partiellement ce problème ? Donc, y a-t-il un espace pour des solutions techniques ?

RAM MOHAN Je vais répondre brièvement, puis Jeff pourra prendre la parole.

Je ne sais pas s'il y a une solution technique, mais je pense que l'on peut faire preuve de pédagogie. Lorsque vous êtes victime d'hameçonnage, est-ce que vous savez comment y réagir ? C'est-à-

dire comment ne pas se faire prendre, mais comment notifier le problème au sein de notre communauté ?

L'un des problèmes principaux, c'est que si l'on ne notifie pas cet hameçonnage ou de l'hameçonnage par SMS, eh bien, vous n'êtes pas capable d'avoir des informations précises quant à la façon dont on a traité un tel pourcentage du problème, puis ensuite de voir qui était responsable de cette partie de l'hameçonnage ou de l'hameçonnage par SMS.

Il faut vraiment pouvoir analyser davantage les caractéristiques de ces utilisations au sein de notre écosystème. Donc il faut vraiment avoir une composante pédagogique importante, et il faut mettre l'accent sur le signalement de l'hameçonnage, de toutes ces questions. Et une fois que ces infractions sont signalées, on pourra utiliser ces données. Et ces données nous permettront de bien cibler les espaces problématiques ou cibler potentiellement les individus qui alimentent ces problèmes.

Pour l'instant, l'on tente d'avoir une approche un peu trop englobante qui s'applique à tout le monde. Ou alors on a tendance à mettre tout un groupe d'acteurs dans le même panier, alors que vous pourriez avoir des acteurs dans ce groupe qui font un travail excellent et d'autres qui font un travail catastrophique. Une fois qu'on a les données, eh bien, c'est là qu'on pourra dire quelles sont les bonnes pratiques. On pourra dire quelles sont les normes qu'il faut observer. Et je pense que l'on peut mettre en place de bonnes pratiques sans pour autant élaborer des politiques.

Évidemment, il y a des éléments que l'on peut mettre en place pour renforcer l'hygiène sur le Web ou pour renforcer l'écosystème, c'est certain.

JEFF BEDSER Moi, je n'ai rien à ajouter.

NICOLAS CABALLERO Merci Ram. La République dominicaine.

AMPARO ARANGO Merci. Je vais parler en espagnol. Je représente la République dominicaine.

Il s'agit d'un panel très important, très technique, extrêmement technique. Mais je crois que finalement vous traitez de ce à quoi nous sommes confrontés dans nos pays. Et ici, je parle comme gouvernement, représentante gouvernementale d'un petit pays, la République dominicaine.

Et à la fin de votre intervention, on vous disait qu'est-ce qu'on doit faire? Qu'est-ce qu'on doit faire, nous, comme gouvernement ? D'abord, il faut savoir quelle est la situation dans nos pays, au niveau de nos opérateurs de registre.

Moi, je viens du secteur réglementaire — réglementation des noms de domaine. Donc quelles sont nos réponses vis-à-vis de ces attaques ? Parce que, ces dernières années, nous avons eu énormément de problèmes. Le Costa Rica, il y a quelques années,

a dû essuyer un nombre d'attaques impressionnant qui lui a coûté des millions de dollars.

Donc, de notre point de vue, nous, gouvernements, et je sais que c'est difficile pour vous de le dire de but en blanc comme ça, mais je pense qu'on a besoin de stratégies d'orientation plus claires pour savoir comment promouvoir le DNSSEC dans nos pays. Combien d'acteurs connaissent le DNSSEC ? Combien en ignorent l'existence ? Que ce soit nos administrateurs, bureaux d'enregistrement, opérateurs de registre, etc., le connaissent ? C'est ça, le cœur du problème. Et c'est ainsi qu'on va pouvoir aborder la question de la cybersécurité, qui est un véritable fléau.

Donc, j'aimerais savoir quelles sont vos recommandations. Mais je vois que ça, ça va pouvoir se faire entre le SSAC et le GAC, parce que tous vos conseils, on va devoir ensuite les transformer, les traduire en outils concrets, réglementation, outils concrets. Mais tout ça, c'est coûteux, disposer de systèmes dotés du DNSSEC.

J'essaie de vous livrer une réflexion que j'ai et qui m'angoisse. C'est pourquoi je voulais vous en faire part. Et je crois qu'on a les outils nécessaires pour pouvoir atténuer ces impacts. Merci.

RAM MOHAN C'est vraiment une question cruciale. Alors, l'un des défis au sein du SSAC, c'est que l'on peut fournir toute une série de savoir-faire technique et d'informations techniques. Mais en revanche, ce que l'on ne comprend pas pleinement, ce sont vos besoins et le niveau

auquel vous avez besoin d'informations. Je pense qu'il faut que nous collaborions afin de comprendre les informations dont vous avez besoin.

Et l'un des éléments que nous avons commencé à mettre en place est le suivant. Nous avions pour habitude de faire le travail et de publier des rapports extrêmement techniques qui allaient de 10 à 40 pages. Et l'un des éléments que l'on a commencé à faire, c'est de faire des résumés exécutifs de ces rapports, qui expliquent en réalité le cœur du rapport.

Mais tout cela ne se concentre que sur ce que l'on estime important. Et ce que je vous encourage à faire, c'est de venir nous parler. Nous sommes ravis de collaborer directement avec vous. Mais en règle générale, vous, membres du GAC, collaborez avec nous. Fournissez-nous davantage de perspectives sur deux éléments : 1) le type d'information qui vous est utile, et 2) le niveau de détail technique dont vous avez besoin.

Notre approche par défaut, c'est de baigner en plein dans le technique -- la technique. C'est pour ça qu'on est là. On est des experts techniques. Mais si vous voulez qu'on survole un petit peu, eh bien, vous pouvez nous le demander et on le fera.

NICOLAS CABALLERO Amparo, c'est une ancienne main ou… Il faut que l'on boucle. Nous avons une minute. Y a-t-il une ultime question du GAC ? Le Japon ? Merci.

JAPON

Vous avez mis l'accent sur l'importance de recueillir des données quant aux utilisations malveillantes du DNS afin d'avoir des informations statistiques. Mais il y a d'autres utilisations malveillantes, telles que CSAM, où il y a également les atteintes au droit d'auteur qui entravent la croissance économique. Mais je pense que la cause profonde est similaire.

Faut-il corriger tous ces types d'utilisations malveillantes ? Mais comment le faire en collaboration avec les gouvernements ?

RAM MOHAN

Je pense que c'est un sujet important. Nous sommes prêts à vous épauler pour vous fournir les conseils techniques, les informations techniques pour mieux collaborer. Mais je pense qu'en fin de compte, la solution, eh bien, prendra la forme d'une association du volet gouvernemental, du volet technique et du volet politiques, qui trouveront ensemble un moyen d'agir ensemble au sein de cet espace.

NICOLAS CABALLERO

Merci beaucoup Ram. Nous devons boucler notre session. C'était une session fantastique.

Ram, comme à l'accoutumée, c'est un plaisir de t'avoir ici. Même si, pour certains, cette conversation peut paraître un peu technique, mais on essaie de faire passer le message. En tout cas, tu fais de ton mieux pour faire passer le message, pour nous donner de bons

conseils d'une part et d'autre part nous aider à lutter contre les méchants. Merci Russ. Merci Ram. Tu as une équipe vraiment fantastique, et j'espère que l'on pourra organiser une autre session à Prague. Merci. On peut les applaudir, nos amis du SSAC. Merci.

Et la session est close. On se voit demain à 9 h pour la cérémonie de bienvenue et pour la cérémonie d'excellence de la communauté.

[FIN DE LA TRANSCRIPTION]