ICANN73 | Forum virtuel de la communauté – Séance plénière : faire évoluer la conversation sur l'utilisation malveillante du DNS
Mercredi 9 mars 2022 – 10h30 à 12h00 AST

BRENDA BREWER : Nous allons donc commencer. Bonjour à tous. Bienvenue à cette séance plénière de l'ICANN 73, « Faire évoluer la conversation sur l'utilisation malveillante du DNS ». Je m'appelle Brenda Brewer, et je suis responsable de la participation à distance.

Veuillez noter que cette séance est enregistrée et suit les normes de conduite de l'ICANN.

Pour garantir la transparence de la participation dans le modèle multipartite de l'ICANN, nous vous demandons de vous inscrire dans les séances de Zoom en utilisant votre nom, par exemple, prénom et nom de famille. Vous risquez d'être sorti de la réunion si vous ne vous inscrivez pas en utilisant votre nom.

L'interprétation pour cette séance inclut l'arabe, le chinois, le français, le russe et l'espagnol. Cliquez sur l'icône interprétation dans la barre de menu de Zoom pour sélectionner la langue que vous préférez.

Pendant cette séance, les questions ou les commentaires envoyés dans le chat ne seront lus à haute voix que s'ils sont insérés dans le format adéquat que j'ai noté dans le chat. Je lirai les questions et commentaires à voix haute au moment choisi pour la séance.

Pendant cette partie de la discussion de la communauté. Si vous souhaitez prendre la parole, veuillez cliquer sur « Lever la main » sur la barre de menu de Zoom. Avant de parler, veuillez éteindre les notifications de tous vos dispositifs et ne parlez pas trop vite pour être bien interprété. Une fois que le facilitateur de la séance aura appelé votre nom, vous aura donné la parole, veuillez mettre en route votre micro et donner votre nom pour l'enregistrement.

Pour voir la transcription en temps réel, vous pouvez cliquer sur *Closed captioning*, dans la barre de menu de Zoom.

Et maintenant, bienvenue au modérateur de cette séance, Graeme Bunton. Vous pouvez commencer.

GRAEME BUNTON : Merci, Brenda. Bonjour ou bonsoir à tous et merci d'être avec nous pour cette plénière d'aujourd'hui. Donc faire évoluer la conversation sur l'utilisation malveillante du DNS, sur les enregistrements détournés ou l'enregistrement à des fins malveillantes.

Je m'appelle Graeme Bunton. Je suis responsable du DNS Abuse Institute. Et la première chose que je souhaite faire, c'est m'excuser pour la longueur de l'introduction.

Le sujet est complexe. Nous avons beaucoup de panélistes, et nous devons quand même bien vous décrire le contexte. Donc, un petit peu de patience, s'il vous plait.

Donc nous allons d'abord écouter Maciej, qui va nous donner une

introduction beaucoup plus robuste du sujet. Mais pendant cette introduction que moi je vais faire, je souhaite en fait bien établir les bases.

Donc voilà un petit peu ce que nous allons faire aujourd'hui. Pour être très simple, la séance a pour objectif d'observer les différences entre les processus d'atténuation pour les domaines enregistrés à des fins malveillantes délibérément et les domaines qui ont été détournés ou piratés et qui sont également utilisés pour nuire.

Donc dans une situation, vous avez quelqu'un qui délibérément essaie de faire quelque chose de mauvais avec un nom de domaine, et dans l'autre cas, non. Et donc il faut bien comprendre quelle est cette complexité dans le cas de l'écosystème.

Donc avant d'entrer dans le vif du sujet, il y a plusieurs choses en termes d'objectifs de cette séance. Donc je vais vous dire un petit peu comment la conversation sera structurée.

Donc Brenda, est-ce que je peux avoir la deuxième diapositive, s'il vous plait ? Merci.

Les objectifs de la plénière. Voilà, ce que nous allons essayer de faire aujourd'hui dans les quelques minutes que nous avons. Nous allons essayer d'élaborer une bonne compréhension au sein de la communauté sur le pourquoi de cette distinction et pourquoi elle est importante. Nous allons également parler du comment, comment pouvons-nous faire la distinction. Donc les problèmes techniques. Nous n'allons pas rentrer trop dans le vif du sujet à ce niveau-là. Mais ensuite,

et là, je crois que c'est vraiment le cœur du sujet. Nous souhaitons élaborer une bonne compréhension au sein de la communauté sur ce que l'on peut faire dans les deux situations. Donc enregistrement malveillant ou détournement. Et enfin, nous parlerons des activités potentielles, qu'est-ce qu'on peut faire, quel est le rôle de la communauté et qui peut agir.

Donc voilà, passons maintenant au cadre. Et c'est important.

Je suis à l'ICANN depuis beaucoup trop longtemps maintenant. Je suis impliqué dans beaucoup de plénières, et je crois qu'il y a un lien entre la spécificité des sujets et ce que l'on retient des séances telles que celle-ci. Donc je souhaite vraiment que tout le monde ici comprenne bien qu'il faut cibler ce dont nous parlons aujourd'hui. Il y a certaines hypothèses qui sont nécessaires dans le cadre de cette conversation. Et donc ce dont on parle ici, c'est un bureau d'enregistrement ou un opérateur de registre qui a reçu un rapport d'abus. Donc, comment ce rapport est arrivé, peu importe dans le cadre de cette discussion. Nous allons partir du principe que l'abus a été vérifié, qu'il y a quelque chose qui est mauvais et qui réellement se passe. On ne va pas parler de savoir si, oui ou non, il y a eu quelque chose de nocif. Nous allons surtout nous concentrer aujourd'hui sur les programmes malveillants et l'hameçonnage.

Tout le monde a sa propre définition de l'utilisation malveillante du DNS, mais ce n'est pas de ça que nous allons parler. Donc je souhaite être très clair. Nous n'allons pas aujourd'hui rentrer dans toute la discussion de la définition de l'utilisation malveillante du DNS, ce que

c'est et ce que ce n'est pas. Nous sommes là pour vraiment comprendre la distinction entre les enregistrements à des fins malveillantes et les enregistrements de domaines qui ont été détournés.

Donc ensuite, dans le cas de cette conversation, nous allons vraiment essayer de nous limiter à ce sujet. Nous allons essayer de voir quels sont les commentaires qui ne sont pas forcément dans le cadre ou dans la mission pour voir ce qu'on peut faire à l'avenir, mais je vais vraiment être très strict par rapport à nos objectifs dans la discussion.

Vous avez l'option d'envoyer vos commentaires ou questions dans la fenêtre présentée à cet effet. Et je vous demande donc de bien rester fidèle à cette définition de la session que j'ai donnée, donc de ne pas sortir de la discussion.

Alors, voilà un petit peu la carte qui va nous guider. Nous avons donc un signalement d'abus auprès d'un bureau d'enregistrement ou d'un opérateur de registre.

La première question, c'est pourquoi est-ce qu'il faut faire la distinction ? Est-ce qu'il s'agit d'un processus d'abus générique ? Et si on n'est pas d'accord et qu'il faut faire la distinction, eh bien, il faut voir comment. Comment est-ce que l'on distingue ? Quels sont les attributs de l'enregistrement qui vont nous mener à faire ce choix ? Et ensuite, nous avons deux possibilités. Nous avons le processus dont il faudra parler pour les domaines enregistrés à des fins malveillantes, donc ceux qui délibérément souhaitent nuire. Et ensuite, il y a l'autre processus pour les sites qui ont été détournés, et qu'est-ce qu'on fait par rapport à ça.

Alors, je crois que ce qui est vraiment épineux et difficile dans le cas de cette conversation, c'est le processus des sites détournés. Et c'est à ça qu'il nous faut réfléchir au sein de la communauté. Donc, nous en parlerons également.

Alors nous avons à un panel très intéressant. Nous allons commencer par une introduction de Maciej, qui est professeur à l'université de Grenoble, Grenoble qu'il faut bien prononcer en français. Il va nous donner des données pour bien comprendre un petit peu le contexte. Ensuite nous passerons à la discussion de notre panel. Et avec nous, nous avons des personnages illustres. Merci à tous d'être avec nous. Nous avons Lori Schulman de l'unité constitutive de la propriété intellectuelle, Chris Lewis-Evans du groupe de travail de la sécurité publique du GAC, Alan Woods du groupe des parties prenantes, donc des registres, Reg Levy pour les bureaux d'enregistrement et Rod Rasmussen du SSAC.

Donc il y aura deux parties à cette séance. Premièrement, nous allons donc faire l'introduction et nous parlerons un petit peu des enregistrements à des fins malveillantes et des enregistrements qui ont été détournés. Et puis, il y aura un moment pour les questions du public. Mais en fait, dans le cas de toute cette conversation, je vous encourage à utiliser la fenêtre questions-réponses, en faisant attention parce qu'il faut vraiment rester concentré sur le sujet dont nous débattons aujourd'hui. Donc si votre question ne trouve pas de réponse, c'est qu'elle correspond à une discussion ultérieure. Donc ne soyez pas déstabilisés si votre question ne correspond pas au sujet de la séance d'aujourd'hui.

Voilà ce que je voulais en termes d'introduction. J'espère que nous avons maintenant des attentes claires, des objectifs clairs et un cadre clair. Voilà donc, nous pouvons maintenant lancer le débat.

Ceci étant, je vais donc passer la parole à Maciej, qui va nous présenter, de manière générale, ce qui se passe dans le domaine des enregistrements à des fins malveillantes. Maciej, allez-y.

MACIEJ KORCZYNSKI : Merci, Graeme, pour cette introduction. Bonjour à tous.

Aujourd'hui, je vais brièvement parler du problème des enregistrements à des fins malveillantes et des enregistrements détournés ou noms de domaine détournés. Cela est basé sur un projet de recherche financé par AFNIC et SIDN. Et je vais également parler de la question technique en faisant référence à l'étude de l'Union européenne sur l'abus du DNS.

Donc vous voyez en haut, ici, une URL qui a été mise sur la liste noire par Phish Tank. Et vous voyez ici un site malveillant. Donc la question à laquelle nous cherchons à répondre, c'est de savoir si ce domaine a été enregistré à des fins malveillantes.

Donc, pour répondre à cette question, nous devons faire une petite investigation de cette situation. Lorsque nous nous rendons sur ce nom de domaine, il n'y a pas de contenu illégal. Et lorsqu'on regarde bien quelles sont les informations WHOIS, on voit que l'enregistrement a été fait deux jours avant que le l'URL soit mis sur liste noire. Donc dans ce cadre, cela veut dire qu'il y a preuve. Il y a enregistrement malveillant.

Et donc le contenu est illégal ou abusif.

Donc du point de vue technique, c'est l'opérateur de services DNS, donc l'opérateur ou le bureau d'enregistrement et le fournisseur d'hébergement. Alors pourquoi est-ce que c'est aussi important en termes d'atténuation ? Parce que l'attaquant pourrait enregistrer un autre nom de domaine. Si on interrompt l'hébergement sans bloquer le nom de domaine, le nom de domaine pourrait être réutilisé dans le cadre d'autres attaques et de campagnes d'hameçonnage. Donc pour augmenter les obstacles et pour augmenter le cout économique, il faut que les choses soient faites au niveau du DNS et au niveau technique.

Ensuite, donc autre cas. Ici, nous avons un autre nom de domaine. Pardon, une autre URL malveillante sur liste noire. Et nous voyons ici la page. Donc même question. Est-ce qu'il y a enregistrement malveillant ? Lorsque nous nous rendons sur le nom enregistré, il y a un site Web avec un contenu légitime, et le contenu correspond également au nom de domaine en lui-même. Lorsqu'on regarde les informations WHOIS, le nom de domaine a été enregistré en 2014. Et donc, le nom de domaine en lui-même est sans doute légitime. Lorsqu'on regarde l'URL malveillant, on peut voir des indices. On peut voir *wp-includes*. Donc cela veut dire qu'il y a eu exploitation d'installations vulnérables. Donc le nom de domaine est légitime ; le site a été détourné à des fins de contenu illégal ou abusif. Donc hameçonnage d'identifiant et atteinte aux marques.

Donc d'une manière générale, il ne revient pas au bureau d'enregistrement ou à l'opérateur de registre de bloquer, parce que

cela pourrait engendrer des dommages pour donc la partie commerciale. Et donc, l'atténuation doit être au niveau de l'hébergement, par le fournisseur d'hébergement ou par l'administrateur du site Web.

Il y a deux choses à faire : premièrement, de nettoyer le contenu malveillant et également d'utiliser un patch pour l'installation vulnérable. Et qui doit s'en charger ? Eh bien, c'est soit le fournisseur d'hébergement, par exemple sur une plateforme de partage d'hébergement où le fournisseur contrôle tout le logiciel, y compris le logiciel vulnérable, ou alors au niveau de l'administrateur Web si l'hébergement n'est pas géré et si c'est l'administrateur qui contrôle le logiciel vulnérable dans ce cas.

Donc, comment est-ce que les domaines légitimes font l'objet d'abus ?

Selon notre analyse, on s'est aperçu que les domaines sont surtout l'objet d'abus au niveau du site Web. Donc il y a un logiciel qui est exploité, par exemple au niveau des adresses. Parfois, ça se produit au niveau du DNS. L'exemple, ici, c'est celui du *domain shadowing*, où les attaquants essaient d'abord d'hameçonner les identifiants du titulaire de nom de domaine ou du bureau d'enregistrement pour obtenir leur enregistrement. Et une fois qu'ils sont connectés, ils peuvent ajouter des sous-domaines qui pourraient être utilisés lors, disons, d'attaques d'hameçonnage.

Diapo suivante, s'il vous plait.

Alors quelles sont les approches existantes pour faire la distinction

entre les noms de domaine légitimes et détournés, et les noms de domaine malveillants et ceux qui ont été détournés.

Donc il y a plusieurs approches.

La première se base sur l'euristique qui est issue de rapports dans ce secteur. Donc d'abord, l'âge du nom de domaine, comme on l'a expliqué auparavant, le temps entre l'enregistrement et le moment où c'est mis sur liste noire, également les modèles. Par exemple, dans le cadre de campagnes d'hameçonnage, quels sont les services qui sont ciblés.

Et deuxième type d'approche, les approches d'apprentissage machine. Et là, le premier exemple c'est COMAR, qui a été développé par une université. Il s'agit d'une approche totalement automatique. L'idée, c'est de collecter des données liées au cout, lié au site Web, à la structure de l'URL. On détermine des noms de domaine spécifiques, etc., et en extrait 38 caractéristiques. Il s'agit d'une approche totalement automatique, fondée sur une modélisation, avec un taux de précision de 97 %.

Alors quel est le rapport entre le type d'abus et les noms de domaine détournés ou malveillants.

Ici, on voit la distribution entre nom de domaine détourné et malveillant. En bleu détourné et en rouge malveillant.

D'une manière générale, l'attaquant doit contrôler le DNS. Toutefois, pour ce qui est de logiciels malveillants et d'hameçonnage, ça n'est pas le cas. L'attaquant peut utiliser les noms de domaine détournés. Et ici,

environ 25 % des noms de domaines qui font l'objet d'hameçonnage et 41 % de noms de domaine qui sont distribués de manière malveillante, vous le voyez ici à l'écran.

Donc, quelle est la variation entre les différents types de TLD ?

Dans la deuxième partie de 2021, on s'est aperçu que pour les nouveaux gTLD, près de 98 % des domaines étaient considérés comme enregistrés de manière malveillante. Si on regarde les ccTLD européens, sur la gauche, on s'aperçoit que 41 %, des noms de domaine a été catégorisé comme détourné.

Et quels en sont les motifs ?

Il s'avère qu'au sein des ccTLD de l'Union européenne, nous avons moins d'enregistrement spéculatif, plus de sites Web de plein droit, qui ont déployé des logiciels qui peuvent s'avérer vulnérables, et donc, les attaquants s'en servent pour attaquer ces sites Web.

Vous voyez ici les variations entre les différents TLD.

Excusez-moi. Je crois que nous avons perdu la connexion ; je ne vois plus la présentation à l'écran.

GRAEME BUNTON : Si, on vous entend. C'est revenu. C'est la diapo 13. Elle est à l'écran.

MACIEJ KORCZYNSKI : Oui. J'essaie de la retrouver. Excusez-moi. Donc, là voici.

Donc, vous voyez ici, je vous le disais, le nombre total de noms de domaine, noms de domaine ayant fait l'objet d'abus par les différentes TLD. Les enregistrements malveillants. En particulier, dans la dernière colonne, vous voyez le pourcentage d'enregistrement malveillant pour tous les noms de domaine qui abusent de TLD particuliers.

Vous voyez ici pour certains TLD, on voit le pourcentage d'enregistrement de noms de domaine malveillant près de 100 %.

Pour mentionner. TK, ici, les noms de domaine sont offerts de manière gratuite aux utilisateurs, et ça, c'est du pain béni pour les attaquants.

On voit également les TLD, par exemple. BR, avec 34 % d'enregistrements de noms de domaine malveillant. Et ça, ça peut s'expliquer par différents facteurs. Et là, j'aimerais attirer votre attention sur le fait que ces résultats doivent être interprétés avec prudence en raison de la limite des classifications, mais aussi en raison des limites des listes noires elles-mêmes qui pourraient ne pas représenter l'ensemble de l'espace cybernétique, étant donné que certains fournisseurs de liste noire peuvent se limiter par rapport à certains noms de domaine en identifiant certains mots-clés, par exemple.

Et une chose qui me semble importante de dire ici aussi, c'est que ce que l'on voit sur la liste noire peut-être différente aussi par rapport à ce que voient les TLD dans leur *helpdesk,* lorsqu'ils analysent et examinent les plaintes des victimes de ces attaques. Pourquoi ? Parce que ces listes noires peuvent ne pas être représentantes de l'ensemble des attaques.

Et enfin dernière remarque. Parfois, on voit des variations plus ou moins importantes pour le même TLD. Par exemple. INFO ou. COM, d'un mois sur l'autre, les choses changent. Pourquoi ? Une raison possible, c'est que l'un des revendeurs, par exemple, offre de grandes réductions aux noms de domaine exploités par les attaquants. Et dans ce cas-là, on voit une augmentation dans le pourcentage de noms de domaine malveillant par rapport au nombre total. Ou par exemple, parfois, on voit certaines vulnérabilités qui sont découvertes et qui affectent des centaines de milliers de noms de domaine. Et là aussi, c'est du pain béni pour les attaquants qui peuvent les exploiter à l'échelle. Et à très court terme, on voit une réduction dans le pourcentage de noms de domaine malveillant par rapport au nombre total.

Voilà. Merci beaucoup de votre attention et j'espère que ces informations et cette présentation vous auront aidés et vont pouvoir lancer la conversation.

GRAEME BUNTON : Merci, Maciej. En fait, dans votre présentation, vous avez déjà répondu à un certain nombre de questions qu'on va aborder par la suite.

Il y a eu beaucoup de questions à l'attention de Maciej, et par rapport à plusieurs choses, notamment l'approche et l'apprentissage machine, etc. Alors je ne sais pas si on va rentrer dans le détail de la manière dont on peut procéder. Mais peut-être qu'on peut voir quelles sont les différentes caractéristiques des noms de domaine et quels sont les outils qu'on peut utiliser, ou quels sont les outils qui sont utilisés par les

humains lorsque cette technologie n'est pas en place.

Maciej, est-ce que vous pourriez répondre ?

MACIEJ KORCZYNSKI : Oui.

Par rapport à la première question. On a fait une analyse de l'importance des fonctionnalités dans la classification COMAR. Alors comme je l'ai dit au début, il s'agit d'un apprentissage machine totalement automatique qui fonctionne sur la base d'un algorithme. Et ces fonctions, ces caractéristiques sont très utiles et sont basées sur le contenu. Par exemple, si on a un site Web avec différentes technologies qui sont utilisées pour créer ce site Web, ça, c'est une indication que le site Web a été détourné. Si on voit dans le cas de PayPal qu'il y a un certain type de vérification, et on a vérifié aussi ce genre de mots-clés, ça, c'est une indication du fait que ce nom de domaine a été enregistré de manière malveillante.

Et enfin, cette classification et les technologies qui sont beaucoup plus difficiles pour les hommes. Mais d'un autre côté, si on veut les faire de manière manuelle, alors il y a un certain nombre de choses à prendre en considération. C'est ce qu'on a vu dans l'exemple que je vous ai présenté ; le temps qui s'écoule entre l'enregistrement et le moment où ce site Web est mis sur liste noire. Si ce temps est très court, alors c'est une indication du fait que le nom de domaine a été enregistré à des fins malveillantes. S'il n'y a pas de contenus significatifs sur le site Web, alors ça, c'est une autre indication que le nom de domaine a été

enregistré à des fins malveillantes. Et ces deux exemples sont de bons exemples qui nous montrent que l'être humain et l'approche d'apprentissage machine peuvent tous deux détecter ce type d'agissements.

GRAEME BUNTON : Parfait. Merci, Maciej. Alors je vois qu'il y a beaucoup d'activité sur le chat. Mais écoutez, je vous invite à utiliser l'onglet questions-réponses pour poser vos questions, parce qu'il y a trop d'échanges sur le chat. C'est impossible de le suivre.

Bien. Il y a beaucoup de questions sur la détection. D'abord le DNSAI a publié un document très intéressant à ce sujet. Vous avez indiqué le lien sur le chat. Et il y a une présentation.

Il y a une présentation lundi, journée Tech, sur ce sujet. Mais on va passer du comment, ça a été intéressant avec les technologies et les approches humaines, pour décider de savoir si un enregistrement a été fait à des fins malveillantes ou pas. Mais on va passer maintenant au pourquoi, et ça va être ma première question à l'attention des membres du panel.

Est-ce qu'on devrait faire cela ? Est-ce que ça fait sens de vérifier nos processus d'atténuation ? Est-ce qu'il faut faire la différence entre les enregistrements détournés et les enregistrements à des fins malveillantes ? Est-ce qu'on devrait appliquer une approche généralisée ou spécifique ?

Alors si tout le monde est d'accord avec cette question, est-ce qu'on

devrait traiter tous les abus de la même manière ?

Voilà, je m'en tiens là. Voyons qui veut rapidement réagir à cette question, répondre à cette question au panel. Reg, allez-y.

REG LEVY : Oui, tout à fait. Il est absolument nécessaire de faire cette distinction. On a beaucoup de clients qui sont des créateurs de sites Web commerciaux, qui font des mises à jour régulières, et s'ils ne font pas de mise à jour régulière, alors ils sont vulnérables au détournement. Donc on prend contact avec les titulaires de nom de domaine pour leur dire qu'il faut faire quelque chose avec leurs sites Web qui ont été créés il y a 10 ans, ils n'ont rien fait depuis.

Et donc, les gens voient leur mail sur leur site Web. Et ça implique tout un processus. Il faut s'assurer que leur activité n'est pas en danger parce que leur site Web a été détourné.

GRAEME BUNTON : Merci Reg. Alors, j'ai Alan, puis Chris, puis Lori.

Alors, n'approfondissons pas trop l'aspect pourquoi, mais plutôt comment.

ALAN WOODS : Très bien. Alors, je pense que oui. C'est très important de faire cette distinction.

Et je sais que la raison qui a été avancée pendant de nombreuses

années, c'est toujours la même. De notre point de vue, du point de vue des opérateurs de registre, il y a beaucoup de dommages collatéraux. Donc on ne veut pas victimiser une autre victime, c'est-à-dire le titulaire de nom de domaine avec un nom de domaine détourné.

Donc il est clair. Si on veut entreprendre des actions, il faut pouvoir faire la différence. Il ne s'agit pas d'une simple nuance, mais d'une différence réelle entre les victimes aussi.

GRAEME BUNTON : Très bien. Merci, Alan. Chris.

CHRIS LEWIS-EVANS : Merci. Juste pour dire que je suis d'accord, on devrait traiter les choses différemment puisqu'il y a une différence.

On a deux sources de dommages ici. D'abord à des fins malveillantes, et ensuite on a un dommage collatéral, le détournement. Et on a deux types de victimes aussi. La première victime, et ensuite celle qui subit les dommages collatéraux. Donc il faut les traiter différemment, ces victimes. J'espère avoir aidé avec cet élément de réponse.

GRAEME BUNTON : Lori.

LORI SCHULMAN : Oui, je voulais dire que l'IPC est d'accord. Il faut absolument faire la distinction, c'est très important, entre les domaines enregistrés à des

fins malveillantes et les domaines contournés.

Et dès le départ, il faut voir comment nous pouvons répondre rapidement aux problèmes. Mais, en même temps, je crois qu'il ne faut pas se perdre dans cette question de distinction, de qui est vraiment la victime, parce qu'il y a l'utilisateur final qui est victime d'hameçonnage ou qui est victime d'une attaque. Mais il y a aussi, en fait, la personne dont la réputation est compromise, dont l'entreprise subit un préjudice. Et donc le titulaire de nom de domaine ne préfère pas nécessairement d'avoir ce site. Il pourra préférer en fait d'avoir ce site peut-être retiré pendant un certain temps si cela peut protéger en fait sa réputation et ses clients.

GRAEME BUNTON : Oui, merci pour cette réponse. Donc il semblerait que personne n'est en désaccord par rapport à cette question. Il faut vraiment faire la distinction ; et donc ça, c'est déjà une bonne chose.

Mais pour nous, c'est plus compliqué. Donc il faut essayer de voir un petit peu maintenant plus profondément ce que cela veut dire. Alors, il y a un certain nombre de questions dans la fenêtre questions-réponses, et on devrait sans doute y répondre avant d'avancer davantage. Donc je vais essayer d'attribuer les questions aux différents panélistes et on va voir comment ça va.

Il y avait une question de Greg Shatan qui, pour moi, me semble être adressé à Maciej. Donc il demandait en quoi est-ce que l'utilisation malveillante au niveau du serveur mail correspond à votre démarche ?

Alors, je trouve que c'est intéressant. Maciej, est-ce que vous pouvez nous dire un petit peu ce que vous en pensez ?

MACIEJ KORCZYNSKI : Au serveur mail ?

GRAEME BUNTON : Oui, je crois que Greg se demande s'il peut s'agir d'hameçonnage ou de programmes malveillants par e-mail.

MACIEJ KORCZYNSKI : Est-ce que peut-être l'auteur de la question pourrait la poser, parce que j'ai besoin d'une clarification ?

GRAEME BUNTON : Je ne sais pas si je souhaite donner la parole, étant donné le format que nous utilisons ; peut-être que Greg pourrait donner des détails dans le chat. Et on y reviendra.

MACIEJ KORCZYNSKI : Merci.

GRAEME BUNTON : Alors, à quoi répondre avant de passer à notre sujet ? Il y a énormément de questions. Donc un petit peu de patience, je suis désolé.

Je vais essayer de voir ce qui correspond au sujet dont nous débattons maintenant.

Autre question de Samaneh. La méthodologie ML et les caractéristiques utilisées dans COMAR, est-ce que ceci inclut également l'euristique mentionnée dans la première étape ? Et donnez des exemples.

MACIEJ KORCZYNSKI : Oui, merci pour cette question. Nous avons inclus toutes les caractéristiques qui sont utilisées donc dans l'euristique dans ces méthodes, à part une, une fonctionnalité, parce que —

Il y a deux raisons en fait. Premièrement, la raison principale, c'est tout simplement que la méthode COMAR doit faire la distinction entre enregistrements malveillants et enregistrements détournés seulement sur la base des données collectées et relatives à un cas spécifique, sans obtenir des enregistrements d'autres domaines enregistrés de façon malveillante. Donc pas des enregistrements groupés. Mais pour le reste, ça va.

GRAEME BUNTON : Merci, Maciej. Je crois qu'il y a une autre question de Michael Palage.

GRAEME BUNTON : Il aimerait connaitre votre opinion sur le haut pourcentage en Europe de ccTLD détournés. Est-ce qu'il est plus facile pour les individus malveillants de détourner un domaine, contrairement à l'enregistrement d'un domaine avec des données frauduleuses ?

Donc si je comprends bien, c'est pourquoi est-ce qu'il y a eu une

augmentation, c'est ça ? En Europe, des noms de domaine détournés.

Alors j'en ai parlé un petit peu dans la présentation. On ne peut que spéculer. Parce qu'en fait on n'a pas pris de mesures. Mais ce que je peux dire, c'est que, dans le cas des ccTLD, nous l'avons déjà mentionné, il y a moins de domaines parqués ; il n'y a pas autant de domaines qui soient spéculatifs. Il y a des sites Web derrière les noms de domaine. Donc s'il y a des sites Web, l'utilisateur s'en occupe et il déploie différents logiciels. Nous envoyons de nombreux qui sont déployés. Et pour certains, c'est tout simplement une exploitation.

Alors la deuxième partie de la question, c'était pourquoi est-ce qu'on voit moins de domaines enregistrés à des fins malveillantes ? Et donc encore une fois, je n'en suis pas certain. Je spécule. Mais il y a beaucoup de ccTLD qui empêchent ces enregistrements malveillants parce que dans les ccTLD, il y a un système similaire, un système qui détecte les enregistrements malveillants. Il y a d'autres ccTLD qui luttent de manière active pour empêcher ces enregistrements malveillants. Mais donc SIDN et AFNIC, par exemple, mais ceci est basé sur mon expérience, sur les recherches que je vois, les graphiques que je vois au niveau des ccTLD, mais ça dépend en fait des ccTLD. Il y en a d'autres qui procèdent peut-être différemment.

GRAEME BUNTON : Merci, Maciej. Alors, il y a beaucoup de questions dans le chat. Nous allons faire de notre mieux pour bien les suivre. N'hésitez pas – donc ceci s'adresse aux panélistes – si vous souhaitez répondre à une question, soit dans le chat des questions, soit en live. Mais je crois qu'on

pourrait peut-être passer maintenant à la gauche du diagramme, donc parler du processus d'enregistrement malveillant et des différentes considérations par rapport à ça.

Donc nous avons décidé qu'il serait bon de faire la distinction. Nous avons un petit peu vu comment ces décisions pourraient être prises, les attributs des noms de domaine, le ML, ou alors c'est la personne qui le fait, et maintenant, qu'est-ce qu'on fait ? Passons à cette partie-là.

Au niveau du bureau d'enregistrement et opérateurs de registre, il n'y a pas beaucoup d'options finalement, mais on pourrait peut-être y réfléchir quand même, et je vais passer pour ceci la parole à Rod.

Rod, est-ce que vous pouvez nous dire ce que vous en pensez ? Quelles sont les activités d'un bureau d'enregistrement ou d'un opérateur de registre ? Qu'est-ce qu'il peut faire s'il y a suspicion d'un enregistrement de ce type ?

ROD RASMUSSEN : Oui. Donc une fois qu'on a déterminé, grâce à une méthodologie sur laquelle on s'est mis d'accord, qu'il y a un problème, alors qu'est-ce que je peux faire ?

En tant que bureau d'enregistrement et opérateurs de registre, nous avons en fait très peu d'options, qui est l'effet escompté, donc d'éliminer le domaine du DNS mondial.

Alors, il y a quand même plusieurs manières de procéder. On peut

simplement effacer, supprimer. On enlève l'enregistrement directement. S'il y a un enregistrement malveillant qui a eu lieu au cours des jours passés, en fait, on peut aussi parler de finances. Donc il y a un avantage, mais il y a aussi un désavantage à ça. Parce que la personne qui a enregistré peut réenregistrer en utilisant le même bureau d'enregistrement. Ou alors un autre. Et tout simplement relancer son enregistrement malveillant.

Lorsqu'il y a un contenu malveillant, c'est une chose, mais il y a aussi le problème des détournements. Ou alors on peut suspendre le domaine sans le supprimer. Donc on utilise le statut de suspension au niveau du DNS. Et donc, quel que soit le délai de l'enregistrement, il y aura donc ce statut de suspension, donc, d'attente et c'est quelque chose qu'il faudra gérer au niveau du bureau d'enregistrement ou de l'opérateur de registre, voire les deux.

Il y a d'autres mesures d'atténuation active qui sont possibles également. Pendant plusieurs années, le groupe de travail de lutte contre l'hameçonnage avait une page d'accueil, et donc on pouvait rediriger. Par exemple, si c'était de l'hameçonnage, on pouvait rediriger, changer le DNS et donc ajouter ceci sur cette page d'hameçonnage. Donc, pour le programme malveillant, il y a une méthode qui permet d'informer les victimes que leur machine a été détournée. Donc, ça, c'est fait de plusieurs manières, soit directement par les fournisseurs, par les sociétés de sécurité, par les agences d'application de la loi, etc. Donc, on peut de manière très active informer les victimes de l'infection par un programme malveillant de leur machine.

Et à cet effet, il faut parfois transférer le nom de domaine à une autre entité. Donc soit du point de vue du titulaire de nom de domaine, donc par exemple, le FBI saisit un domaine et des transferts ; Microsoft l'a fait très souvent également.

Il y a également une autre option. Il y a le bureau d'enregistrement de dernier recours qui a été mis en place. Et donc c'est pour les domaines de commandement et de contrôle, pour les programmes malveillants.

Donc il y a plusieurs options pour les victimes, mais ceci implique du travail, un processus et de la documentation qui soit prête.

Et dernière chose que je souhaite ajouter, lorsque vous avez déterminé que l'enregistrement est malveillant, eh bien, il est bon d'essayer de voir s'il n'y a pas d'autres domaines qui sont alignés pour être utilisés potentiellement par le même titulaire de nom de domaine par ce compte. Donc regarder ce qui se passe dans ce compte. C'est très important, je crois. Et je pense qu'on pourra peut-être écouter mes collègues, mais voir comment le compte a été mis en place par l'acteur, comment il a été détourné. Quels sont les domaines qui ont été ajoutés, pour voir s'il y a un problème de victime ou d'identifiant.

Et enfin, regarder un petit peu les différents modèles ou tendances qui existent sur le compte pour voir s'il n'y a pas eu un abus transversal sur un grand nombre de domaines et de comptes de titulaires de nom de domaine. Parce que là, on aura une campagne de grande ampleur, parce que certains de ces acteurs sont très rusés et ils arrivent à se cacher des bureaux d'enregistrement qui sont sérieux et qui souhaitent les éliminer de leur liste.

GRAEME BUNTON : Merci beaucoup, Rod. C'était très bien. Et il y avait beaucoup d'informations. Donc, je vais faire un petit récapitulatif rapide.

Les bureaux d'enregistrement ont, en fait, trois options. Peut-être plus les bureaux d'enregistrement que les opérateurs de registre, même si ces derniers peuvent participer.

Donc, on peut effacer, on peut suspendre ou on peut rediriger. Et il y a en fait des motifs qui vont correspondre à ces trois options.

Donc on va vérifier le compte. On va voir si le compte correspond à une certaine tendance, et je crois que tout ceci est tout à fait utile pour les personnes qui cherchent à atténuer les abus.

Et j'aimerais bien savoir ce que sorte que Reg et Alan ont à dire. Comment est-ce qu'ils voient les choses, comment déployer ceci. Est-ce que c'est utilisé ? Pourquoi ou pourquoi pas ?

Mais avant, pendant que vous réfléchissez, Lori, c'est à vous.

LORI SCHULMAN : Merci. J'ai une question pour répondre à ce qu'a dit Rod par rapport aux tendances des abus. Est-ce que vous pourriez nous donner des exemples ? Parce qu'aujourd'hui, avec ce qu'on voit, les tendances au niveau législatif et les politiques actuelles, on s'aperçoit que la recherche se limite uniquement à un bureau d'enregistrement. Ou est-ce que les opérateurs de registre peuvent trouver plus de bureaux d'enregistrement. Et est-ce que ça a un sens qu'un opérateur de registre

fasse ce genre d'enquête, plutôt qu'un bureau d'enregistrement ?

GRAEME BUNTON : Merci Lori. Rod ?

ROD RASMUSSEN : Oui j'aimerais répondre à cette question.

Oui, pour répondre à votre question, oui. Les bureaux d'enregistrement ont la capacité unique de voir ce qui a été expurgé par rapport aux informations protégées, etc., et ça, c'est un avantage énorme en termes euristiques, etc., dont Maciej parlait auparavant.

Et ils ont aussi la possibilité de voir d'où viennent les connexions, les cartes de crédit utilisées, etc., donc ils peuvent voir en profondeur les choses. Et un opérateur de registre peut avoir, s'il voit quelque chose de suspect qui a lieu, surtout s'il utilise un algorithme et qu'il y a une série de fonctionnalités prédéterminées pour détecter un commande et contrôle de logiciels malveillants. On voit ça entre différents bureaux d'enregistrement. Il y a une tendance là.

On peut voir aussi ce qui se passe au niveau de l'hébergement du DNS et la manière dont le domaine est configuré sur l'Internet lui-même. Donc si vous regardez la manière dont les principaux serveurs du DNS fonctionnent ou les adresses IP pour hébergement, vous pouvez très souvent détecter ce genre de choses.

En tout cas, si vous avez une suspicion, voilà les choses qu'il faut

regarder. Il faut regarder ce genre de choses pour voir si les choses sont légitimes ou pas.

GRAEME BUNTON : Merci, Rod. Et un petit commentaire pour Chris. Et je vais demander à Reg et Alan d'intervenir avant que vous puissiez répondre.

Mais je me demande – par rapport au détournement, je me demande si du point de vue des autorités, est-ce qu'en général pour vous, est-ce que vous préférez un détournement plutôt qu'un enregistrement malveillant qui impliquerait une investigation plus profonde, etc.

Alors on va passer à Reg puis Alan. Reg ?

REG LEVY : Reg Levy de Tucows. Nous sommes un bureau d'enregistrement en gros.

Alors notre approche par rapport à cela, qui va être un peu différente de celles d'un bureau d'enregistrement qui a une relation directe avec le titulaire de nom de domaine, on travaille avec les revendeurs.

Donc, lorsqu'on a beaucoup d'abus qui nous viennent de la part d'un revendeur en particulier, on le contacte et on dit voilà, on est expert en abus du DNS, comment est-ce qu'on peut vous aider ?

Et très souvent, les choses se résolvent d'elles-mêmes, avec ce simple argument. Et lorsqu'on voit qu'il y a une suspicion d'activité malveillante de leur part, on s'adresse directement. Et, comme ç'a été

dit sur le chat, très souvent, ces attaquants n'utilisent pas leur nom ou le même nom pour enregistrer des noms de domaine. Donc utiliser cette tendance ça n'est pas toujours utile.

Ensuite, autre question. Est-ce qu'on regarde quand est-ce que le domaine a été enregistré pour voir si ça a été enregistré à des fins malveillantes aussi si ce nom de domaine a été détourné. Oui, tout à fait. Mais il y a beaucoup d'intelligence artificielle, et il en est beaucoup question sur le chat, qui offre un panorama trop large pour ce qui est du retrait des noms de domaine. Donc il faut voir ce que l'intelligence artificielle nous propose. Ce que j'aime beaucoup raconter, c'est un algorithme. Parce que quelqu'un a réussi à enregistrer un nom de domaine. Et c'était justement la chaine utilisée par un autre. Et c'était leur acronyme pour une petite équipe de football américaine, de femmes en Amérique. Donc voilà ce qu'ils ont voulu enregistrer, mais encore une fois, c'est l'exemple de ce genre d'algorithme qui, finalement, ne nous aide pas vraiment.

GRAEME BUNTON : Merci, Reg, de cette anecdote.

Alors, Alan et Chris. Et je vous demanderais d'être bref pour qu'on puisse avancer.

ALAN WOODS : Oui. Très brièvement. Par rapport au bureau d'enregistrement, c'est comme ça qu'il faudrait procéder. Et tout ce qu'il a dit Reg, il a tout à fait raison. Moi, je parle d'abord à mes bureaux d'enregistrement et je

pense que c'est très important du point de vue des opérateurs de registre.

Oui, effectivement on va regarder ces indicateurs, et certains vont le faire pour moi, mais ensuite il faut que je le transfère au bureau d'enregistrement, pour ensuite avoir une conversation avec les titulaires de nom de domaine.

Donc il y a une conversation qu'on doit avoir ici, parce qu'on parle de détournement. Donc, je pense que c'est un aspect important.

Mais autre chose que je veux dire, du point de vue d'un opérateur de registre, et Lori en parlait pour les petites entreprises. Je pense qu'il faut être très clair là-dessus. Est-ce que le dommage est appliqué davantage aux titulaires de nom de domaine ou au bureau d'enregistrement. Et ça, ça mérite une analyse très approfondie.

[L'interprète s'excuse, mais l'audio d'Alan se coupe.]

GRAEME BUNTON : Merci, Alan. Et ça, c'est très intéressant par rapport à nos discussions. Et je reviendrai là-dessus dans un instant après que Chris ait répondu.

CHRIS LEWIS-EVANS : Merci. Alors, pour en revenir aux noms de domaines enregistrés à des fins malicieuses, oui. En fin de compte, de quoi parle-t-on ? De logiciels malveillants et d'hameçonnage. Donc ça implique des investigations. Et en général, ces gens n'enregistrent pas un seul nom de domaine.

Donc le nom de domaine va faire l'objet d'une investigation et tout ce qui a à voir avec l'opérateur de registre, fournisseur d'hébergement, bureaux d'enregistrement, il faut passer là à un travail proactif, et tout ça, ça va engendrer d'autres victimes et des dommages collatéraux.

Donc ce que font les autorités, c'est justement entreprendre ce genre d'investigation et essayer de limiter les dégâts.

GRAEME BUNTON : Très bien. Merci. Il nous reste encore 35 minutes, et on veut s'assurer de pouvoir répondre à toutes les questions. Il y a énormément d'activité sur le chat. Merci à tous ceux qui participent.

Alors, je pense que jusqu'à présent, on a abordé la partie facile des choses. Est-ce qu'on fait une différence ? On a parlé du comment, et on a parlé avec Rod de ce qu'on doit faire en cas d'enregistrement à des fins malicieuses.

Maintenant, on a l'autre partie du problème, qui se complique un petit peu, à savoir l'exemple d'abus du DNS. Et là, on a l'exemple de logiciels malveillants et d'hameçonnage sur un site détourné.

Donc ça peut être le site d'une petite entreprise ou pas. Mais voilà la conversation qu'il faut avoir maintenant. Alors quel est le processus pour savoir quoi faire dans ce genre de cas.

Peut-être que je vais commencer avec une question un peu provocatrice. Si vous voyez qu'un site Web est détourné, qu'il y a abus du DNS, est-ce que, dans certains cas, vous allez décider de suspendre

le domaine ? En cas de détournement. Alan.

ALAN WOODS : C'est une question intéressante et je pense qu'il faut être très clair, en tant qu'opérateur de registre. Nous, on a une politique très stricte par rapport à la suspension, par rapport au mail associé à ce nom de domaine.

Alors, si je n'ai pas de réponse de la part du bureau d'enregistrement et que le problème subsiste, oui peut-être qu'on va suspendre. Mais vous savez, tout ça, ça dépend des dommages occasionnés.

Excusez – moi les interprètes. Je suis un petit peu emporté par ma passion, donc je vais un peu vite.

Donc, des choses qui portent atteinte à la vie, par exemple, matériel de pédopornographie, des choses de ce genre, alors, les opérateurs de registre ne devraient pas subir les conséquences de cette suspension si on a une autre option.

Alors, on a tendance à utiliser la suspension comme option de dernier recours pour des domaines détournés. Alors on va prendre contact avec le revendeur et le titulaire de nom de domaine, en disant voilà il y a un problème et il faut le régler. Et en fonction de leur réponse ou absence de réponse, on peut commencer à faire un petit historique pour voir d'où vient le détournement, à quoi il remonte.

Parfois ça, ça fait que les gens s'aperçoivent que c'est important. Et ça déclenche une action de leur part. Et ça, c'est une autre partie du

problème. Parfois, on doit permettre la résolution du domaine pour que les gens puissent se connecter à leur nom de domaine.

Donc suspendre le nom de domaine, ça va résoudre le problème des fins malveillantes, mais ça ne va pas résoudre le problème de l'atténuation ni de l'utilisation de ce nom de domaine.

GRAEME BUNTON : Merci. Alors Lori, Rod ou Chris. Je me demande s'il y a des informations qui, d'après vous, devraient être incluses dans cette évaluation des couts et dommages. Est-ce que ça devrait être pris en considération lorsque les gens doivent analyser ce qu'ils vont faire avec leur nom de domaine détourné ?

LORI SCHULMAN : Oui, Graeme, si vous le permettez, je vais répondre d'abord en raison des échanges sur le chat. Parce que moi aussi j'ai participé à ces échanges. Il y a une grande conversation en cours.

Alors, lorsque vous regardez les noms de domaines détournés, vous ne cherchez pas toujours une série de faits préétablis. Parce que lorsque vous regardez un domaine détourné, vous avez plusieurs choses à faire. Que faire ? Comment faire ? Parce que lorsque vous offrez un service, alors suspendre ce domaine, ça ne va pas résoudre le problème.

Ce que j'essaie de dire, et pour répondre à Rod et à Alan, de quoi parle-t-on lorsqu'on parle de logiciels malveillants et hameçonnage, lorsqu'on parle de sites détournés et de pédopornographie ?

Le cas très clair, et moi je l'ai vu dans ma propre activité, un site est détourné, et j'en reviens aux petites entreprises et non pas aux grandes entreprises, parce que là encore, les grandes entreprises ont leurs propres procédures. Mais pour les petites entreprises, c'est différent. Peut-être que ces petites entreprises vont décider on n'a pas besoin de ça. On a besoin du CSAM. Voilà ce que je veux dire.

Vous ne pouvez pas avoir une solution qui réponde aux besoins de tous. Et excusez-moi, je parle trop vite. Je vais ralentir tout de suite et je m'en excuse. Je viens de la côte ouest des États-Unis. Je m'en excuse.

Donc ce que je vous dis plus lentement, c'est qu'il y a des décisions nuancées qui doivent être prises par rapport aux domaines détournés. On ne peut pas faire des hypothèses par rapport à ce qu'un propriétaire d'entreprise veut faire ou ne veut pas faire. Et dans certains cas, ce sont des mesures extrêmes, mais il ne faut pas prendre de décision sans en informer les autres.

Et j'apprécie beaucoup ce qu'a dit Tucows par rapport à la communication qu'ils ont avec leurs revendeurs. Tout ça, ça dépend du dommage engendré. Et on a également la prise en considération du titulaire de nom de domaine qui pourrait décider dans son propre intérêt de suspendre le nom de domaine pour le vendre, pour que leur propre marketing et leur propre publicité autour du domaine ne soit pas diluée. C'est un terme marketing que j'utilise là, mais en tout cas que leur renommée ne soit pas entachée par ce détournement de domaine.

GRAEME BUNTON : Merci Lori. J'ai Chris, Alan et ensuite j'ai une question que je souhaite poser au panel. Donc Chris.

CHRIS LEWIS-EVANS : Merci. Je crois qu'en ce qui me concerne, par rapport aux domaines malveillants, le groupe des bureaux d'enregistrement et des opérateurs de registre a fait un excellent travail par rapport aux normes requises, par rapport à leur avis. Et ce travail n'a pas été fait pour les domaines détournés.

Donc pour que les bureaux d'enregistrement et les opérateurs de registre puissent agir, il faut qu'il y ait des preuves. Donc davantage d'explications sur la situation du domaine détourné. Et donc, il faut qu'il y ait le contact de la société, contact du bureau d'enregistrement, et que rien n'ait été fait.

Et donc la discussion revient au préjudice subi.

En ce qui concerne les programmes malveillants, il y a beaucoup d'articles dans ce domaine et l'infection, par exemple de rançon logicielle, ça peut signifier la fin d'une entreprise et la perte de beaucoup d'emplois.

Donc pouvoir articuler ceci dans le cadre de normes claires ; nous avons beaucoup travaillé avec Amotech qui ciblait et nuisait à de nombreuses entreprises. Nous avons pu articuler ceci. Nous avons contacté le titulaire de nom de domaine. Nous avons pu le dire. Nous avons contacté le fournisseur de service, rien ne s'est passé. Donc maintenant, nous venons vers vous, bureau d'enregistrement,

opérateur de registre, pour une suspension, à cause de ça. Et donc cela veut dire que le processus a permis la décision.

Et nous comprenons également que, parfois, il faut qu'il y ait une discussion. Il s'agit d'une grande société multinationale pour laquelle on demande la suspension, donc l'impact est massif. En fait, cette campagne d'hameçonnage ne cible que quelques personnes, et donc, l'impact sera massif. Donc, essayez de nous donner 48 heures et on va réfléchir à la réponse.

Donc il y a eu beaucoup de conversations, de communication. Et ceci réduit beaucoup le préjudice qui est subi et le dommage collatéral. Donc c'est vrai, cela demande davantage de preuves de ceux qui signalent, mais c'est également quelque chose qui nécessite davantage d'implication de ceux qui font partie de la chaine qui, donc, prendra les mesures.

GRAEME BUNTON : Merci, Chris. Donc beaucoup de choses dans votre intervention.

Je pense que vous avez tout à fait raison. Il y a énormément de travail à faire dans cet espace. Et il y a aussi la question des responsabilités, de l'expertise des bureaux d'enregistrement et des opérateurs de registre. En ce qui concerne les services d'hébergement, on y reviendra, mais d'abord Alan.

ALAN WOODS : Oui, après Chris, je n'ai plus grand-chose à dire.

Une des choses qui finalement nous aident tous les deux, c'est le SSAC115 en termes d'opérabilité pour s'assurer que l'opérateur est impliqué au bon moment pour que la réponse soit opportune. Parce que l'objectif, ici, c'est le délai. Plus on effectue les choses de manière opportune, moins l'impact est important.

Donc on peut aussi considérer les efforts du DNS Abuse Institute, et donc effectuer tout ce travail en amont. Mais une des choses que je souhaite noter également, c'est que certains titulaires de nom de domaine, bien sûr, sont des titulaires de grandes plateformes qui ont des procédures de surveillance d'abus très importantes. Donc par exemple, Facebook.com, etc., on ne va pas évidemment éliminer Facebook. Donc il faut faire l'équilibre.

[L'interprète s'excuse ; nous avons des problèmes pour entendre cet intervenant.]

GRAEME BUNTON : Donc il y a une question qui s'est posée à plusieurs reprises, et je vais la reposer donc à Reg, parce que je crois que ceci correspond à quelque chose d'important.

Donc, quelle est la relation que vous avez avec les sociétés d'hébergement, vous, bureaux d'enregistrement et opérateurs de registre. Parce qu'il me semble qu'il y a plusieurs personnes qui pensent que cette relation est étroite. Je ne vais pas parler en votre nom, mais je crois que dans certaines circonstances, ce n'est pas le cas. Et donc on parle de la complexité du sujet. Chris a parlé des chemins

d'escalade entre les différents acteurs. Est-ce que ces relations sont claires ? Est-ce qu'il y a des normes de processus ou alors est-ce qu'il faut travailler là-dessus ? Reg ?

REG LEVY : Merci, Graeme. Et encore une fois, ma réponse va partir du fait que Tucows est surtout un bureau d'enregistrement de revente. Donc la réponse pourra être différente pour d'autres.

Nous n'avons pas de services d'hébergement. Il y a 500 sites là-dessus, des filiales. Donc à la base, ce que je peux vous dire, c'est que nous n'avons pas. C'est tout ce que je peux vous dire.

Nos revendeurs sont également des sociétés d'hébergement, donc très souvent nous pouvons les contacter et leur dire, il y a eu un détournement sur ce site. Et c'est eux qui s'en chargent. Ça veut dire que le titulaire de nom de domaine n'est même pas impliqué. Donc si notre vendeur est une société d'hébergement, nous avons cette relation. Et c'est une relation étroite. Mais ce n'est pas toujours le cas.

Et il y a beaucoup de sociétés d'hébergement —

Alors, l'hébergement, c'est un service qui nécessite un nom de domaine, mais qui est complètement séparé des services d'enregistrement de noms de domaine. Et donc, dans le cas où le revendeur n'est pas la société d'hébergement, là, c'est moins clair. Et il faut utiliser un outil, voir qui est la société d'hébergement comme n'importe quel utilisateur final. Et en fin de compte, on peut contacter la société d'hébergement, mais c'est plus compliqué.

GRAEME BUNTON : Merci Reg, et je vais passer la parole à Alan avant de poursuivre.

ALAN WOODS : Merci encore une fois. Mes excuses pour les interprètes. Je sais que je parle vite.

Donc du point de vue de l'opérateur du registre, c'est beaucoup plus compliqué. Nous n'avons pas vraiment ce lien avec les fournisseurs d'hébergement. Pour nous, c'est quelque chose qui doit être fait avant ; c'est ce qu'on pense. Avant que ça nous arrive.

Et on essaie de voir si le bureau d'enregistrement peut faire ce lien, s'il est également fournisseur d'hébergement. Mais ce que je peux dire, c'est que nous essayons quand même d'établir une relation avec eux en dehors de tout ça. Donc il y a plusieurs conversations de toute évidence. Et une des conversations, c'est les contacts à l'ICANN, mais il y a également la juridiction de l'Internet dont nous sommes membres. Parce que dans le cadre de cette discussion, il y a des fournisseurs d'hébergements qui sont dans la discussion, mais finalement ils ne sont pas tous dans l'ICANN. Donc il faut entrer en contact avec eux, faire le pont. Et je crois que c'est important pour nous, cependant, de retirer tous ces enseignements que nous avons en dehors, de les ramener dans la communauté de l'ICANN.

Nous le faisons de plus en plus. C'est ce qui se passe et c'est comme ça que la définition sur la juridiction de l'Internet est venue au niveau des parties contractantes. Donc, nous essayons de travailler avec eux et de

ramener ceci à la communauté, parce que c'est important pour nous, pour les bureaux d'enregistrement et pour les opérateurs de registre également.

GRAEME BUNTON : Merci, Alan. J'ai l'impression que beaucoup de beaucoup de bureaux d'enregistrement sont hébergeurs, mais après, la relation avec les sociétés d'hébergement dépend. Il y a le nombre réparti dans le monde. Et donc ce n'est pas toujours si clair. Et donc il faut essayer de clarifier ces processus de signalement avec les sociétés d'hébergement, voir comment clarifier les choses, et ensuite, quelles sont les voies de communication pour les opérateurs de registre et les bureaux d'enregistrement s'il n'y a pas de réponse du côté du titulaire par rapport à un certain nombre de postes. Et donc voilà un petit peu ce qu'on pourrait faire.

Alors Lori, je vois que vous avez la main levée. Il nous reste 18 minutes.

Donc après, nous parlerons des questions qui ont été mises sur Zoom.

LORI SCHULMAN : Oui, je voulais faire un suivi par rapport à ce qui a été dit dans le chat. J'essaie de suivre autant que je peux.

Mais en termes de signalement et d'interopérabilité, je crois qu'il faut absolument mentionner —

[Problème de connexion. Désolée. L'interprète s'excuse.]

Alors, par rapport à ce que disait Reg, il y a le travail dans le domaine de l'intelligence artificielle. Les résultats sont inspectés. Donc, nous comprenons bien – en tout cas, mon unité constitutive comprend bien qu'il faut investir pour davantage de sécurité dans le domaine de l'Internet.

Et dans certains cas, cela veut dire des prix supérieurs. Est-ce qu'on veut vraiment parler de ça ? Donc c'est une question pour la société civile, parce qu'est-ce qu'on souhaite réellement que cet espace d'accès aux domaines reste abordable ? Nous savons qu'il y a certains opérateurs de registre et bureaux d'enregistrement qui investissent davantage, et est-ce que cela paye ? Est-ce que ce ne serait pas une question qui serait intéressante, et que la communauté devrait se poser ?

GRAEE BUNTON : Merci Lori, je pense que c'est une bonne transition par rapport aux autres questions et par rapport à ce qui se passe dans le chat et dans la fenêtre questions-réponses. C'est quel est le rôle de la communauté, le rôle de l'ICANN, pour essayer de répondre à certains des enjeux que nous avons découverts ici. Peut-être qu'il pourrait y avoir de meilleures pratiques du point de vue des enregistrements à des fins malveillantes. Quel est le rôle de l'ICANN, pour tout ce qui est détournement ? Donc quel est le rôle de la communauté ?

J'ai beaucoup de choses à dire de mon point de vue, du point de vue de mon institut, mais je laisse ça de côté. Ce que j'aimerais savoir de la part du panel, c'est qu'est-ce que vous pensez ? Quelle est l'orientation à

prendre dans la communauté ?

Donc, n'hésitez pas à lever la main. Reg, je vois que vous l'avez déjà fait. Allez-y.

REG LEVY : Oui, je crois vraiment que l'équipe de conformité de l'ICANN a une mission. Du point de vue des contrats, ils doivent absolument être respectés. Lorsqu'une mesure n'a pas été prise pour lutter contre l'utilisation malveillante du DNS. Donc lorsque quelque chose fait partie de la mission de l'ICANN, lorsqu'on ne parle pas de pédopornographie ou de contenus, mais qu'on parle bien d'abus, eh bien, l'abus du DNS, l'ICANN doit absolument exploiter ceci et s'assurer que les contrats sont respectés.

GRAEME BUNTON : Merci Reg. Rod et ensuite Chris.

ROD RASMUSSEN : En fait, il y avait une question similaire dans l'onglet questions-réponses à laquelle j'ai répondu.

Alors, le SSAC a parlé de cela dans le document SSAC115. Et là, il y a un rôle de l'organisation ICANN et de la communauté ICANN en général, pour participer à cette conversation. Et d'ailleurs, la conversation doit être beaucoup plus large.

En fait, l'abus du DNS, c'est une sous-catégorie de tous les abus qu'il y

a. Et certains des défis qu'on a évoqués aujourd'hui par rapport au fait de savoir quels sont les fournisseurs de services pertinents qui doivent être impliqués pour atténuer les préjudices et faire la différence entre les enregistrements malveillants et les enregistrements détournés, ça aussi c'est une excellente conversation.

On peut également parler de normes, en termes de preuves, quelles sont les attentes par rapport à la reconnaissance, et l'atténuation en termes de rapports et d'abus. Bref, des choses un peu plus larges.

On voit que, dans cette direction, on a des initiatives telles que l'étude ou la création du DNSAI, l'Institut sur l'abus du DNS. Et donc il y a beaucoup d'efforts qui sont réalisés pour créer de meilleures pratiques, des normes, etc., mais on n'y est pas encore et il y a encore beaucoup de chemin à parcourir pour essayer de créer un écosystème où les gens pourraient avoir des attentes par rapport au processus, à la proportionnalité.

Et tout ce dont vous avez besoin pour avoir une meilleure réponse est de mettre en place un système préventif pour éviter les abus.

Et donc, pour arriver jusque-là, il est important que la communauté ICANN soit sur la même longueur d'onde et s'engage avec la communauté plus large de l'Internet pour voir comment aborder ces questions. Parce que si, chacun dans son coin, on essaie de trouver une solution, on va finalement créer beaucoup de systèmes parallèles. Et peut-être que l'ICANN, ce serait le meilleur endroit pour susciter cette conversation puisque l'ICANN dispose des ressources nécessaires de la capacité de sensibilisation et de convocation nécessaire.

Voilà. Je vous encourage à regarder le document SSAC115 et à être aussi proactif que possible, et de manière plus générale penser à la manière dont on peut régler ces problèmes et au type de cadre dont on aurait besoin pour fixer certaines attentes et les atteindre.

GRAEME BUNTON : Merci. Je pense que quelqu'un mentionnait justement le SSAC 115 sur le chat. Mais il est bon de le nommer de nouveau.

CHRIS LEWIS-EVANS : Bien. D'accord, je suis tout à fait d'accord avec ce que vient de dire Rod.

Et ce que je voulais dire justement, c'est que j'étais d'accord avec ce qu'a dit Reg par rapport à la conformité.

Mais je pense qu'on a beaucoup avancé pour savoir comment faire face à l'abus du DNS. Dans cette conversation, on a des processus en place pour y faire face, pour faire face au détournement des sites et avoir un niveau minimum d'attentes. Tout cela permet à la conformité de mesurer les réponses. Ça, ce serait très utile. Et d'avoir également des normes ou des outils à la disposition des opérateurs de registre et bureaux d'enregistrement pour qu'ils comprennent bien de quoi il s'agit. Bref, des outils d'éducation. Parce qu'il y a toute une kyrielle d'opérateurs de registre et de bureaux d'enregistrement. Et donc il faut que tout le monde soit sur la même longueur d'onde et sache de quoi il s'agit.

Donc l'ICANN peut faire beaucoup pour diffuser ce message dans tout

le paysage de l'ICANN et faire un travail de sensibilisation auprès des entreprises de services, entreprises d'hébergement. On a beaucoup parlé au cours de cette conversation.

GRAEME BUNTON : Merci, Chris. Alan, et ensuite on va essayer de répondre à quelques-unes des questions posées sur l'onglet questions-réponses.

ALAN WOODS : Très brièvement. Alors, dans ce processus, et avant même d'avoir suggéré cette plénière, le sous-groupe sur l'abus du DNS, du RySG, s'était penché sur cette question. Et ce serait une excellente chose que Rod et les gens du SSAC nous rejoignent autour de cette conversation pour faire justement ce que Chris vient de dire. C'est-à-dire essayer de jeter les bases de cette conversation. Ça a toujours été une conversation ouverte. Il y a clairement un problème par rapport à l'abus du DNS. On continue à y travailler.

Mais il y a des nuances aussi à apporter dans cette conversation. Et ça, ça va nous aider à travailler de manière plus efficace.

Et on espère que très prochainement l'on verra les résultats. Mais en tout cas, c'est un très bon début. Début très prometteur.

GRAEME BUNTON : Très bien. Merci. Et d'ailleurs, c'est avec la TPH qu'on est en train de travailler sur cette question sur un document. Et entre maintenant et l'ICANN 74 à La Haye au mois de juin, on va certainement publier cela.

Ça sera très certainement avant l'ICANN 74, au mois de juin.

Alors, il y a une question sur le chat sur le fait de savoir que peut faire la communauté, quels changements au RAA peut appliquer la communauté pour inclure toutes ces bonnes pratiques et tout ce dont on parle aujourd'hui. Et éventuellement, je pense que c'est sur la table, j'ai reçu au DNSAI une lettre me posant cette question, justement. Et j'y réfléchis moi-même un peu. Et je pense que le rôle de la communauté, aussi, c'est d'essayer d'avoir une approche plus ciblée par rapport à cette conversation très générale.

Peut-être qu'il faudrait commencer par ce qui est le plus simple et évident par rapport à l'aspect malveillant, où les conséquences sont plus limitées et il y a moins de victimes qui sont impliquées. Donc on pourrait commencer à réfléchir à ce que peut faire la communauté du côté des enregistrements à des fins malveillantes. Donc ça, ça serait ma suggestion et j'espère que j'ai répondu ainsi à la question posée sur le chat.

Il nous reste encore sept minutes et j'aimerais voir s'il y a certains membres du panel qui souhaitent dire un dernier mot ou si quelqu'un souhaite répondre directement aux questions qui sont posées.

REG LEVY : Oui, je voulais insister sur quelque chose qui était dit sur le chat.

Le RySG travaille actuellement sur un outil qui va indiquer toutes les informations par rapport au fait de savoir qui est la société d'hébergement et comment les contacter. Donc, soyez attentifs. Ça

devrait être disponible cette semaine, et ce sera très utile.

GRAEME BUNTON : Merci Reg. C'est intéressant. Et d'ailleurs nous, au DNSAI, on travaille sur quelque chose de semblable. Il est clair que ce genre de processus qui consiste à identifier toutes les composantes dans l'écosystème, savoir qui ils sont, comment les contacter, quelles sont les normes, etc., tout ça est un peu brouillon pour l'instant. Et on pourrait mieux faire pour mettre un peu d'ordre dans tous ces processus.

Pour ma part je travaille sur ce genre de choses. Je ne sais pas si c'est un bon endroit pour en parler. Mais en tout cas, sachez que je le fais.

Alors que pensez-vous si on essaie de répondre à deux ou trois questions très rapidement ? Excusez-moi. On n'a pas le temps de répondre à toutes les questions.

Alors au panel, est-ce que vous avez quelque chose à ajouter par rapport à ce dont on a parlé aujourd'hui ? Lori a levé la main, allez-y.

LORI SCHULMAN : Merci. Je n'arrive plus à suivre le chat. Ça va trop vite. Mais je crois que ce panel est très opportun. Et je souhaiterais remercier les organisateurs qui ont invité l'IPC et moi-même parce que ça met le doigt sur les points les plus complexes.

Ça n'est pas un sujet simple. Je pense que personne ne dit qu'on devrait se précipiter et prendre des décisions. Mais je pense que surtout par rapport au détournement de nom de domaine, la communauté est

confrontée à des spécialistes en matière de sécurité, etc., mais chaque type d'abus fait appel à un remède qui est meilleur ou pire. Et chaque abus fait appel à un certain nombre de faits qui sont différents.

Donc il faut établir des normes et c'est là que les projets de l'ICANN, comme l'I & J, le SSAC115 et ce que vous faites, Graeme, ça nous aide à fixer ces normes justement. Mais l'étape suivante, et je pense qu'il est approprié de le dire, comment est-ce que les normes qui sont établies en dehors de la communauté peuvent fonctionner à l'intérieur de l'ICANN aussi ?

Et j'ai inscrit une suggestion sur le chat, dont on a parlé au sein de mon unité constitutive. Que s'est-il passé, il y a 20 ans, lorsqu'on a commencé à parler de cybersquattage, et comment faire face à ce genre de cas ?

Et on a finalement pu développer l'UDRP qui a très bien fonctionné pendant 20 ans. Est-il temps, maintenant, de penser à un processus de type UDRP pour ce qui est du détournement des sites ? Tout est bon à apprendre. Parler des normes, des processus, etc.,

GRAEME BUNTON : Très bien. Lori, merci beaucoup.

Je voulais brièvement, avant de céder la parole à Alan, répondre à une question de Griffin ; je crois qu'on y a répondu partiellement. Par rapport au travail au sein de la communauté.

Mais étant donné que je suis à la tête d'un institut consacré à cette

question, je vous dirais que, pour moi, il est clair que les questions liées à l'abus sortent très rapidement de la portée de l'ICANN. Et donc il faut être en contact avec les sociétés d'hébergement. Et on travaille sur des processus semblables et sur des solutions semblables.

Ce qu'il faut voir, c'est comment travailler tous ensemble de manière collective. Je pense que tous ensemble, on soutient le modèle multipartite à l'ICANN, et on voit bien l'importance de ce travail.

Mais ce qu'il faut comprendre aussi, c'est qu'il y a une place pour les organisations qui peuvent être en dehors de la mission d'ICANN et engager toute la communauté. Donc pouvoir expliquer que ce soit aux personnes chargées de la règlementation dans le monde, pouvoir donc expliquer à l'industrie comment développer et élaborer les meilleures pratiques, aux fournisseurs de courriers électroniques. C'est à ce genre de personne qu'il faut parler de nos problèmes.

Il ne nous reste plus qu'une minute. Alan, je crois, vous allez avoir le mot de la fin.

ALAN WOODS : Oui. Je voulais reprendre à mon compte ce que vous venez de dire, Graeme. Je pense que c'est important. Et je ne suis pas en désaccord avec ce qu'a dit Lori. De fait, je suis d'accord avec la plupart de ce qu'elle a dit.

L'UDRP, à l'époque, réglait un problème lié aux noms de domaine. Mais aujourd'hui, on fait face à quelque chose de beaucoup plus large. Et donc il faut travailler également avec les bureaux d'enregistrement et

opérateurs de registre, société d'hébergement, en dehors de l'ICANN. C'est beaucoup plus large. Donc, il faut travailler tous ensemble pour essayer d'avancer sur cette question.

Et aujourd'hui, on comprend bien que c'est un domaine interopérable. Il faut tout ce qu'on soit engagé. On arrive à mieux le comprendre, mais il faut continuer à améliorer les choses. Merci.

GRAEME BUNTON : Merci, Alan. Alors, écoutez. Il est l'heure.

Merci à tous les membres du panel. Merci d'avoir pris le temps de venir avec nous, merci à Maciej de votre excellente présentation. Merci aux participants. Merci d'avoir respecté les membres du panel. Et merci de toutes vos contributions.

On va voir si on peut organiser une autre séance ou un autre travail.

Sur ce, nous sommes arrivés à la fin de cette séance. Merci à tous de votre participation et de votre engagement. Merci.

[FIN DE LA TRANSCRIPTION]