ICANN71 | Forum de politiques virtuel – Séance plénière : Comprendre la liste de réputation et de blocage
Jeudi 17 juin 2021 – 10h30 à 12h00 CEST

BRENDA BREWER : Cette séance va commencer. Veuillez lancer l'enregistrement.

Bonjour. Bienvenue à cette séance plénière de l'ICANN71 « Comprendre les listes de réputation et de blocage ».

Je suis Brenda Brewer et je suis la responsable de cette séance. Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendu de l'ICANN.

Pendant cette séance, les questions ou commentaires ne seront lus à haute voix que s'ils sont soumis dans la fenêtre de questions et réponses. Je les lirai à haute voix pendant le temps alloué par le président ou le modérateur de cette séance.

Le service d'interprétation simultanée sera disponible en anglais, en chinois, en français, en russe, en espagnol et en arabe. Cliquez sur l'icône d'interprétation dans Zoom et sélectionnez la langue que vous souhaitez écouter pendant la séance.

Si vous souhaitez prendre la parole, veuillez lever la main dans la salle Zoom et lorsque le modérateur de la séance dira votre nom, notre équipe technique vous permettra d'activer votre micro. Avant de prendre la parole, assurez-vous d'avoir sélectionné la langue dans laquelle vous allez parler dans le menu d'interprétation. Veuillez

indiquer votre nom pour l'enregistrement et la langue dans laquelle vous allez parler si vous parlez une autre langue que l'anglais.

Au moment de prendre la parole, veillez à mettre en sourdine tous les autres dispositifs et les notifications. Veuillez parler clairement et à un rythme raisonnable pour permettre une interprétation exacte de vos propos.

Tous les participants à cette séance peuvent faire des commentaires dans le chat. Veuillez utiliser le menu déroulant du chat et sélectionnez « Répondre à tous les panelistes et participants » ; cela permettra à tout le monde de voir votre commentaire.

Veuillez noter que les discussions privées ne sont possibles qu'entre les panelistes dans le format « Zoom Webinar ». Tout message envoyé par un paneliste ou un participant à un autre participant sera également vu par les hôtes, co-hôtes et autres panelistes de la séance.

Pour accéder à la transcription en temps réel, cliquez sur le lien « Closed Captions » dans la barre d'outils Zoom.

Je vais maintenant donner la parole à LG Forsberg.

LG FORSBERG : Merci Brenda.

Je suis LG Forsberg et je serai le modérateur pour cette séance de l'ICANN71 « Comprendre les listes de réputation et de blocage ». Pour ceux qui ne me connaissent pas, je suis responsable de noms de domaine de Suède et je suis gestionnaire de la partie technique du

côté du bureau d'enregistrement et je m'occupe de plusieurs parties techniques. Je suis technicien et je travaille comme consultant pour différents bureaux d'enregistrement. Et finalement, je suis le fondateur et le curateur d'un système suédois qui s'appelle Nordic Domain Days.

Pendant cette séance aujourd'hui, nous allons travailler avec le public. Nous avons préparé plusieurs questions auxquelles vous pourrez répondre tout en écoutant cette discussion. Deux de ces questions vont être présentées maintenant et les suivantes seront posées dans la deuxième partie de notre séminaire.

Est-ce que vous pouvez s'il vous plaît présenter les questions à l'écran ?

BRENDA BREWER : Merci.

Vous devriez voir la première question sur l'écran.

« Est-ce que vous connaissez les types suivants de menaces contre la sécurité ? » Vous avez les différents types qui incluent parmi les options le spam, le hameçonnage, les logiciels malveillants, le dévoiement, les réseaux zombies, autres.

Nous allons maintenant fermer ce sondage et nous vous donnons quelques secondes pour y répondre. Merci. Nous pouvons retirer le sondage de l'écran. Merci. Et nous passons à la question 2 de ce sondage s'il vous plaît.

« Est-ce qu'un nom de domaine que vous gérez a connu ce type de menaces contre la sécurité ? » Vous pouvez répondre pas oui, non, je ne sais pas ou je ne gère pas de domaine ; vous avez donc quatre options pour répondre à la question « Est-ce qu'un nom de domaine que vous gérez a déjà connu ce type de menaces contre la sécurité ? » : oui, non, je ne sais pas, je ne gère pas de nom de domaine.

Je vous donne cinq secondes pour répondre à cette question. Merci. Nous pouvons retirer la question de l'écran et donner les réponses.

LG, je vous donne la parole.

LG FORSBERG : Merci Brenda.

Je vais continuer. Je vais vous faire une petite présentation du sujet avant de passer à la partie de la présentation du panel.

Aujourd'hui, nous avons différents participants que nous allons associer à cette liste de réputation et de blocage dont nous allons parler aujourd'hui. Ces participants sont l'ICANN, qui fournit les tests et qui contrôle les gTLD ; nous avons aussi des parties contractantes sous la forme de bureaux d'enregistrement et de registres qui vont contrôler leurs TLD, leur liste de noms de domaine ; nous pouvons avoir aussi des fournisseurs de service comme des compagnies d'hébergement qui peuvent utiliser ces listes de réputation et de blocage pour maintenir les courriels de leur clientèle en bonne sécurité et pour rapporter les cas de hameçonnage ou de logiciels malveillants ; finalement, nous avons les utilisateurs finaux qui sont

les titulaires de nom de domaine ou les opérateurs de noms de domaine ou de sites internet qui sont les groupes qui aujourd'hui ne veulent pas avoir une relation avec une liste de réputation et de blocage parce que cette liste de réputation et de blocage signifie plusieurs choses en fonction du groupe auquel ils s'adressent. Pour l'ICANN, pour le registre, pour le bureau d'enregistrement, ce sera un outil utilisé. Et pour l'utilisateur final, ce peut être une signification de désastre si votre courriel est envoyé à ce type de liste de réputation et de blocage – vous aurez à ce moment un écran de Google rouge qui va s'afficher sur votre ordinateur.

De nouveau, la liste de réputation et de blocage est quelque chose qui est intégré dans la discussion du DNS. Nous n'allons pas parler de cela pendant 90 minutes. Nous n'allons pas parler de la définition de l'utilisation malveillante du DNS, mais nous voudrions expliquer ce que sont ces RBL, comment elles fonctionnent, comment les parties contractantes, les fournisseurs de service et les utilisateurs finaux peuvent travailler avec ces listes de réputation ou RBL.

On a beaucoup parlé de ces RBL, mais je dirais qu'on pourrait dire qu'une liste de réputation et de blocage est un recueil de normes de comportement et que la partie de réputation signifie qu'il y a des manières de déterminer si un nom de domaine peut figurer dans une liste ou pas. C'est parfois simplement une réponse de oui ou non. Par exemple, s'il s'agit d'un spam, chaque nom de domaine qui commence par 0 va avoir des points négatifs s'il fait des choses négatives et des points positifs s'il faut des choses positives.

Par exemple, le nom de domaine va être listé dans une liste de blocage et cette partie va être mise en œuvre dans des serveurs de courriels et dans les protections en général pour éviter le trafic. Donc la mitigation de l'utilisation malveillante de ces noms de domaine – excusez-moi – cette lutte contre l'utilisation malveillante n'est pas seulement le premier cas que l'on va trouver. Certaines listes de réputation et de blocage vont donner une liste d'informations complètes concernant les ressources qui ont été découvertes alors que d'autres listes vous donnent seulement une idée que quelque chose de négatif a lieu dans un endroit particulier sur le réseau.

Il y a certaines choses que les listes de réputation ont en commun et c'est la compréhension de la façon dont elles font les choses, ce qu'elles font et ce qu'elles veulent faire pour aider les utilisateurs, ce qui n'est pas toujours facile à comprendre, surtout si vous êtes un utilisateur final qui ne connaît pas ce type de ressources. Mais on peut essayer de comprendre comment ces listes de réputation collectent les données et comment on crée ces listes, comment les utiliser.

Pour ce faire, on a réuni des représentants des listes de réputation et de blocage aujourd'hui qui vont nous parler et on a aussi des représentants des différentes parties que j'ai présentées il y a quelques instants pour nous parler aussi de leurs propres expériences avec les listes de réputation et de blocage. Je vais donc présenter notre premier participant aujourd'hui et je vais lui donner la parole. Il va nous présenter la compagnie pour laquelle il travaille. Je vous donne la parole.

CAREL BITTER : Bonjour à tous. Je m'appelle Carel Bitter de Spamhaus. Je suis impliqué dans ces listes RBL et nous nous focalisons sur les noms de domaine. Nous fournissons des informations sur ce sujet depuis plus de 10 ans. J'ai bien sûr participé à beaucoup d'autres réunions ICANN au préalable. Je suis heureux d'être là pour aider et pour répondre aux questions que vous puissiez avoir.

LG FORSBERG : Merci Carel.

Monsieur Roman Huessy s'il vous plaît.

ROMAN HUESSY : Je suis le fondateur de abuse.ch. Nous travaillons sur tout ce qui est informations des botnet et nous publions ces informations.

LG FORSBERG : Notre dernier participant, il s'agit de monsieur Ben Coon de WMC Global.

BEN COON : Bonjour. Nous faisons fonctionner une plateforme de hameçonnage. Nous fournissons des RBL pour tous les fournisseurs SMS et toutes les personnes menacées dans beaucoup d'instances. Je vous remercie de m'avoir invité.

LG FORSBERG : Merci Ben.

Nous allons continuer avec les discussions. Je voudrais commencer par présenter notre amie Samaneh Tajalizadehkhoob de l'ICANN. Est-ce que vous voulez prendre la parole ?

SAMANEH TAJALIZADEHKHOOB : Oui, merci.

Je travaille au bureau du CTO de l'ICANN au niveau de la sécurité, de la résilience et de la stabilité. J'ai aussi travaillé avec le projet DAAR. J'ai beaucoup d'expérience dans le secteur académique ayant travaillé sur les RBL. Aujourd'hui, je vais parler un petit peu plus de ce que fait l'organisation de l'ICANN dans ce sens et sur ce projet.

Merci.

LG FORSBERG : Je voudrais présenter Matthew Thomas de Verisign. Présentez-vous s'il vous plaît.

MATT THOMAS : Bonjour. Je m'appelle Matt Thomas. Je travaille avec Verisign au niveau de la cybersécurité, de la stratégie et de la recherche. Je suis aussi membre du RSSAC à l'ICANN et je suis vice-président au conseil d'administration de M3AAWG. J'attends beaucoup de ces discussions.

Merci.

LG FORSBERG : Du côté des bureaux d'enregistrement, nous avons Reg Levy de Tucows. Présentez-vous s'il vous plaît.

REG LEVY : Je travaille donc pour Tucows et je suis à la tête du département de la conformité. Je fais partie aussi de l'unité constitutive des bureaux d'enregistrement sur l'utilisation malveillante du DNS.

Bonjour à tous. Il est très tôt chez moi. Je suis vraiment impatient de participer à ce débat.

LG FORSBERG : Merci Reg.

Et en dernier mais non la moindre, de la communauté At-Large, nous avons notre amie Joanna Kulesza.

JOANNA KULESZA : Merci LG. Merci de nous laisser participer et de nous donner l'opportunité de parler de la part des utilisateurs finaux. Je me focalise sur le renforcement des capacités pour l'At-Large et je suis heureuse de faire partie de cette discussion, de participer à ce panel sur les RBL. Quand on regarde les résultats du sondage et quand on voit la participation de la communauté At-Large, nous savons que ce n'est

pas vrai et que les utilisateurs finaux sont bien intéressés par les listes de réputation et de blocage.

Je vous remercie de me laisser participer. Merci.

LG FORSBERG : Maintenant, nous en avons fini avec les présentation et nous allons passer à la première section d'entrevue et là, nous allons parler des RBL et nous allons essayer d'en apprendre plus sur cette thématique. Nous allons demander maintenant à Carel comment nous pouvons résoudre ces problèmes de RBL.

CAREL BITTER : Nous allons parler de la partie blocage. Les listes ne sont pas seulement utilisées pour bloquer. Il y a une autre perspective où les bureaux d'enregistrement et les opérateurs de registre observent les données pour savoir s'il y a des problèmes au niveau des consommateurs ou des utilisateurs. Il ne s'agit pas seulement de bloquer mais d'essayer de remédier au problème.

Des fois, on parle des ensembles de données, surtout dans ce contexte. Donc je pense que c'est une chose importante à distinguer quand on parle de tous les ensembles de données. Que font-elles ? Pourquoi sont-elles utilisées ? Est-ce qu'on les utilise pour la raison pour laquelle elles ont été conçues ? Si ce n'est pas le cas – je ne dis pas qu'on ne pas les utiliser pour faire une chose ou une autre chose –, on doit savoir que chaque utilisation de ces ensembles de données

peut être différente. Donc il faut vraiment bien comprendre comment les systèmes fonctionnent.

Plus le score d'un domaine est haut, plus nous allons savoir si quelque chose de malveillant se produit, quelque chose de négatif. Donc les gens doivent réagir différemment en fonction des scores des noms de domaine. On doit donc comprendre comment les données fonctionnent. Et si ce n'est pas le cas, il faut essayer de rentrer en contact avec les personnes qui créent ces données, donc bien comprendre encore. Vous vous dites : « J'essaie de faire cela », mais est-ce que c'est une bonne idée ? Il y a des choses que vous allez peut-être vouloir bloquer, par exemple dans le contexte des courriels, mais parfois, c'est dans d'autres contextes. Un bon exemple : il y a des problèmes dans des adresses courriels qui utilisent des raccourcis. C'est un petit peu compliqué pour les utilisateurs finaux, donc il faut absolument traiter ce problème.

LG FORSBERG : Merci Carel.

Je voudrais continuer avec deux questions de suivi qui sont spécifiques à Spamhaus. Quelles sont les preuves que nous pouvons trouver pour pouvoir mettre des noms de domaine sur la liste des RBL ? Est-ce que ces preuves peuvent être partagées ?

CAREL BITTER : Dans notre cas, ce n'est pas toujours facile de partager ces preuves. Beaucoup des données que nous recevons viennent de des FSI qui ne

nous laissent pas partager les données. Nous sommes toujours ouverts bien sûr aux questions.

Lorsqu'il s'agit des cas des opérateurs de registre et des bureaux d'enregistrement avec qui nous travaillons, bien sûr, par exemple si nous ne comprenons pas vraiment quelle est la situation, si on a des questions du genre « Est-ce qu'il se passe autre chose ? », il y a des choses que nous partageons, mais ce n'est pas du partage par défaut. Si par exemple on a une liste de 100 noms de domaine, on ne parle pas de 100 logiciels malveillants. Vous savez, c'est une chose que l'on fait cas par cas, à savoir ce que l'on peut partager ou pas.

LG FORSBERG : Roman, qu'est-ce que pensez-vous qui fait la différence, par exemple avec abuse.ch ?

ROMAN HUESSY : Excusez-moi, est-ce que vous pouvez reposer la question ? Je répondais sur Zoom.

LG FORSBERG : Quel genre de preuves d'utilisation malveillante qu'abuse.ch considérerait comme assez fortes ou assez importantes ?

ROMAN HUESSY : Le genre de preuve que nous devrions avoir, le logiciel malveillant qui est utilisé compromettrait des sites et ainsi, cela causerait de sérieux

problèmes. Ce que cela veut dire, c'est que le système vérifie tout ce qui est proposé et si c'est le cas, dans ce cas-là, les preuves sont publiées sur le site web, donc tout le monde peut les utiliser et tout le monde peut les vérifier. Donc le projet est assez transparent lorsqu'il s'agit de fournir ces preuves. Toutes ces preuves sont publiées sur le site web, donc sont rendues publiques.

LG FORSBERG : Merci Roman.

Pour bien comprendre un ensemble de données, est-ce que vous pourriez nous décrire le cycle de vie de celui-ci ? Dans ce cas-là, vous parlez de logiciels malveillants. Par exemple du moment où il vous a été soumis jusqu'au moment où il n'y est plus.

ROMAN HUESSY : Oui. Ce n'est pas comme le phishing. Je m'attends à un certain type de réponse, ce qui veut dire que je peux facilement vérifier les choses, par exemple que le site web héberge encore du contenu malveillant. Une fois que ce contenu malveillant disparaît du site web ou du nom de domaine qui a été notifié, ce que cela veut dire, c'est que l'URL ou le nom de domaine disparaît automatiquement. À cause de cela, la bonne chose, c'est que l'URL reste sur la liste jusqu'à ce qu'il ne soit plus menaçant. Donc nous vérifions plusieurs fois, souvent pratiquement toutes les 10 minutes. Une fois qu'un utilisateur répare cette menace du nom d'URL, nous mettons fin à cela dans l'heure.

Vous savez, plusieurs fois, le contenu malveillant a été retiré, mais il est toujours là au niveau de la racine. Donc notre système va aller vérifier automatiquement si le contenu est encore là. Si c'est le cas, le nom de domaine sera sur la liste une fois de plus.

LG FORSBERG : Merci Roman.

Ben, à vous de prendre la parole. Pensez-vous que ce que Carel et Roman ont décrit ici est différent de façon significative à ce que vous faites dans ce sens en termes de hameçonnage ?

BEN COON : Nous vérifions tous les éléments malveillants avant que ces sites arrivent sur la liste RBL. Nous fournissons une liste de blocage et une liste de vérification automatique. Nous allons tester le site web et nous assurer que tout va bien.

La seule chose différente que nous offrons, c'est que nous ne mettons pas sur la liste des domaines, mais plutôt tout l'URL. Ainsi, on peut voir exactement où se trouve le contenu malveillant. Et ce contenu ne sera plus en ligne. Une fois que l'URL ne sera plus sur la liste, il pourra revenir en ligne.

LG FORSBERG : Repassons la parole à Carel. Vous avez dit tout à l'heure que les personnes utilisant une RBL doivent savoir à quoi sert cette liste. Quelle est l'utilisation la plus importante de cette liste pour

Spamhaus ? Quelle est l'utilisation primordiale ? Est-ce que cela a changé au cours des 10 dernières années ?

CAREL BITTER : Nous travaillons surtout sur la partie des courriels. Je dirais que c'est un petit peu plus compliqué que cela, mais l'ensemble de données que nous publions dans la liste de réputation et de blocage des noms de domaine est notre vision des domaines qui ont une mauvaise réputation. On l'utilise surtout pour les courriels, mais il y a aussi des domaines malveillants, des domaines qui font du hameçonnage, différentes activités frauduleuses. On fait une différence à travers la partie du code DNS et ainsi, il est possible de segmenter une seule partie de ce qui nous intéresse au niveau du hameçonnage ou du logiciel malveillant.

Ce que nous faisons, c'est que nous fournissons des données et nous contrôlons la façon dont les gens utilisent ces données. Nous avons une version gratuite et tout le monde peut l'utiliser. C'est un format qui est utilisé par les serveurs courriels. Vous allez recevoir une réponse qui va vous permettre de faire quelque chose, quelles que soient vos politiques. Il y a des versions qui sont disponibles qui fonctionnent pour différentes menaces et différents cas. Il y a des sous-ensembles qui peuvent être utilisés au niveau des résolveurs de DNS, il y a des systèmes pour les bureaux d'enregistrement et les opérateurs de registre pour la remédiation, pour les enquêtes aussi.

En général, c'est utilisé par les personnes qui doivent prendre des décisions concernant la réputation d'un nom de domaine, mais pour

les courriels. Pour la plupart des noms de domaine, on va pouvoir vous dire s'ils sont utilisés de manière malveillante, donc vous allez pouvoir vérifier. En général, ces courriels sont utilisés à différents niveaux. Et vous allez pouvoir vérifier ces noms de domaine à travers au niveau du résolveur du DNS ou autre.

Les cas d'utilisation que nous avons dépendent des problèmes qu'on essaie de résoudre, comme Ben l'a dit, en fonction des vérifications que l'on veut faire. On voit beaucoup de cas dans lesquels on n'a pas de courriel et c'est plus large qu'une liste de courriels. Si vous avez un problème de sécurité et que les noms de domaine sont concernés, à ce moment-là, il y a des systèmes que produisent Roman et d'autres qui peuvent être utiles pour résoudre ces problèmes et bien comprendre ce qui se passe en réalité.

LG FORSBERG : Merci Carel.

J'ai maintenant une question à poser aux fournisseurs de RBL. Nous avons entendu parler de la façon dont vous recevez des indications de collecte. Vous pouvez dire à ce moment-là qu'en général, on a des détections faites par les machines, d'après ce que vous avez dit. Puis, vous avez les courriels aussi auxquels vous avez accès. Est-ce que vous diriez qu'on a un type d'enquête humaine dans les listes de réputation et de blocage dans vos compagnies ? Est-ce que vous pourriez le dire ? On commence par Ben.

BEN COON : Oui. Nous utilisons un système pour les menaces afin de vérifier les cas de hameçonnage que nous voyons. Nous essayons aussi d'analyser tout ce qui concerne les évaluations de façon à ce que ces problèmes soient directement dans ces listes de réputation et de blocage. Mais nous essayons de vérifier pour qu'il n'y ait pas de faux positifs. À ce moment-là, nous contactons notre équipe et nous essayons de le vérifier. Nous avons donc une série d'interventions manuelles qui se font.

LG FORSBERG : Merci Ben.

Roman.

ROMAN HUESSY : Oui. À propos de notre approche, c'est une approche basée sur la communauté. Les données que je vais utiliser seront seulement une partie des données qui sont à notre disposition.

Quand on parle de la communauté ici qui génère ces données, il y a deux types de rapporteurs. Les premiers sont des utilisateurs que je ne connais pas en qui ne j'ai pas vraiment confiance, donc s'ils nous rapportent quelque chose, nous allons le vérifier manuellement. De l'autre côté, nous avons des rapporteurs en qui nous avons confiance qui vont nous déclarer quelque chose et à ce moment-là, nous allons l'inclure dans notre liste. Néanmoins, notre système va quand même vérifier si le site internet sert un contenu malveillant ou pas.

Maintenant, si vous utilisez une approche de liste de réputation et de blocage, à ce moment-là, le site ou le nom de domaine va apparaître seulement dans la liste de blocage s'il y a un contenu malveillant qui a été présenté. Donc pour répondre à votre question, je dirais que c'est amélioré manuellement en fonction des URL ou des noms de domaine qui sont concernés et qui ont été déclarés pas un système automatique de machines.

LG FORSBERG : Merci.

Carel, allez-y, vous avez la parole.

CAREL BITTER : Dans notre cas, nous utilisons les deux systèmes : une machine et l'humain. Si l'on veut assigner une réputation à tous les noms de domaine qui existent sur la planète, à ce moment-là, il est clair que vous aurez besoin d'utiliser un système automatisé parce qu'il y a trop de noms de domaine, bien sûr. On ne peut pas demander à une personne d'analyser tous ces noms de domaine.

Le système automatisé est bien sûr utilisé, mais nous avons des personnes qui vont analyser les questions qui nous paraissent suspicieuses ou qui vont contrôler des choses qui ne sont pas claires quand il y a des scores qui sont très élevés. Il y a toute une combinaison entre le travail de la machine et le travail humain, bien sûr. C'est une interaction.

LG FORSBERG : Merci.

Nous sommes en train d'arriver au bout de cette première partie de notre séance, mais il y a une question qui sera la prochaine question que je vais vous poser. Comment est-ce que vous définiriez l'indication d'un faux positif dans votre cas ? Quel est le cas le plus courant de faux positif ou le plus récent que vous avez eu ? Ben, allez-y.

BEN COON : Je dirais qu'au niveau des données que nous voyons ayant été rapportées sur les listes noires, il y a toujours des faux positifs. Notre objectif est de diminuer les faux positifs le plus possible.

La principale raison de l'existence de ces faux positifs est le manque de compréhension de ce qui est frauduleux et ce qui ne l'est pas. Nous avons des personnes qui reçoivent quelque chose qui ne leur plaît pas et elles le déclarent comme matériel frauduleux alors qu'elles n'en sont pas sûres par exemple.

LG FORSBERG : Roman ?

ROMAN HUESSY : Oui, il y a bien sûr des faux positifs, il y en a toujours et il y en a toujours eu. Ils peuvent être signalés par tout le monde. Donc si une

personne en qui nous avons confiance nous déclare des sites de hameçonnage, des spam ou autres, on va les exclure du projet.

Je dirais qu'en général, nous avons un bon système d'apport de données, mais il y a bien sûr des erreurs qui peuvent être commises.

LG FORSBERG : Carel ?

CAREL BITTER : Je dirais que des faux positifs, il y en a toujours eu. C'est notre travail de diminuer le plus possible le nombre de ces faux positifs. Je me souviens, il y a plusieurs années, quand on a commencé à avoir ce problème de courriels spams finalement qui n'étaient pas des courriels malveillants, c'était un problème pour les problèmes qui les envoyaient. Dans ce cas-là, on essaie de voir s'il y a un problème qui a été réglé de manière automatique et qui met en jeu la réputation d'un nom de domaine ou d'une adresse IP ou autre. Il y a toujours cette possibilité, surtout si ce rapport a été fait par des personnes qui ne sont pas sûres qu'il s'agisse de hameçonnage ou autres. Pour beaucoup de gens, la différence entre le spam et les courriels normaux n'existent pas beaucoup.

Donc c'est toujours un souci, bien sûr, mais il est clair que si vous y réfléchissez, dans le cas que Roman et Ben ont mentionné, tous les faux positifs qui peuvent surgir dans nos données vont toujours poser des problèmes. On peut ne pas en avoir pendant une semaine et la semaine d'après, vous en aurez trois ou quatre ; c'est normal, c'est la

routine. Le problème, c'est de savoir rapidement régler cela, gérer cette question, l'analyser en profondeur et la résoudre.

Il est clair qu'en tant que fournisseur de données, nous avons nous-mêmes un propre intérêt pour que cela fonctionne correctement. Si les données que nous fournissons ne sont pas correctes, les gens vont arrêter d'utiliser nos services. Donc c'est important aussi dans ce sens.

Je crois que Roman va être d'accord avec moi, les données sont solides si tout le monde les utilise. Par exemple, si vous avez un réseau zombie, plus vite ce nom de domaine est retiré ou plus vite il est bloqué par le plus grand nombre de personnes possible, plus on sera sûrs. Si les gens pensent que nos rapports sont bons, s'ils pensent que nos rapports ne sont pas exacts, on va avoir des problèmes.

Donc nous voulons que les données que nous fournissons soient les plus fiables possibles de façon à ce que le DNS devienne un espace plus sûr pour nous tous. C'est ce que nous amène à faire le travail que nous faisons. Nous essayons de résoudre les problèmes de sécurité pour les bureaux d'enregistrement, pour les opérateurs de registre et nous voulons protéger les utilisateurs finaux. Donc plus les gens utiliseront nos données, plus les gens seront sûrs. Voilà, c'est l'objectif. Ce que nous faisons est quelque chose de très important. On a toujours cela en tête.

Il y a aussi des manières d'être plus agressifs, bien sûr. On peut dire : « Si je fais davantage, je vais bloquer davantage des choses, je vais être plus efficace. » Mais il y a différents scénarios dans lesquels on voit qu'il y a toujours quelqu'un quelque part qui va faire quelque

chose, qui va avoir le même nom pour un hébergement, un URL frauduleux. Donc c'est toujours une question d'équilibre. Il faut être sûr d'essayer d'être aussi bon que possible, de mettre en place un bon processus pour affronter les différents types de problèmes. Par exemple, tout le monde peut entrer dans une liste et retirer un nom de domaine. Vous n'avez pas besoin de remplir un formulaire ou nous contacter par téléphone. C'est un système qui fonctionne comme cela. C'est à notre avantage pour être sûr que les choses soient faites rapidement et que cela puisse être réglé pour les victimes de faux positifs.

LG FORSBERG : Merci Roman.

Nous sommes maintenant à la section questions et réponses. Je voudrais poser une dernière question avant de passer à la prochaine section de la réunion.

Je voudrais demander à Roman si ces listes RBL ont des données originales. Est-ce qu'elles vont coopérer les unes avec les autres ? Par exemple, est-ce que abuse.ch fournit à Spamhaus des données sur ces faux positifs ou fait part des notifications ou des signalements qu'ils obtiennent ?

ROMAN HUESSY : Oui, cette question a été posée auparavant. C'est une question valide.

Il y a bien sûr des processus pour que les informations puissent être partagées avec les vendeurs et les autres. Certains de ces processus sont bilatéraux. Ils existent au sein de Spamhaus ou de Safe Browsing, tous ces fournisseurs de RDL. Mais quand il s'agit de abuse.ch, tout cela est disponible pour tout le monde, tout le monde peut y avoir accès. Il y a une bonne portion de fournisseurs pour les entreprises commerciales qui consument ces données, ces informations. Comme il n'y a pas besoin d'être enregistré, de mon côté, on peut dire que je ne sais pas qui utilise mes informations parce que cela fait partie du domaine public.

Aussi sur le fait de partager des informations sur les faux positifs, je pense que c'est un sujet tout de même important. En ce qui me concerne, je ne pense pas qu'il y ait de mécanismes en place en ce moment sur la façon de signaler ces faux positifs.

Comment je gère cela ? Quand quelque chose est signalé comme était un faux positif, cela sort bien sûr du flux d'alimentation. Donc je vais notifier tous les autres fournisseurs et ainsi, ils pourront retirer ces entrées. C'est quelque chose qui devrait être une thématique sur laquelle on débatte pour qu'on puisse échanger toutes ces informations sur les faux positifs. Peut-être qu'on pourrait annoncer et signaler toutes ces choses et les partager avec d'autres entreprises.

LG FORSBERG : Merci Roman.

Maintenant, nous sommes arrivés au moment de la présentation ICANN de cette séance, donc nous allons passer la parole à Samaneh.

SAMANEH TAJALIZADEHKHOOB : Bonjour à tous. Je suis Samaneh et je représente l'ICANN et le bureau du CTO lors de cette réunion. Je vais parler des listes de réputation et de blocage. Prochaine diapositive s'il vous plaît.

Jusqu'à présent, nous avons eu un très bon débat. Nous avons partagé beaucoup de choses et nous avons couvert déjà beaucoup de choses avec les panelistes.

Je voudrais commencer à la base. Qu'est-ce que sont les listes de réputation et de blocage ? Ce sont des listes de blocage d'IP ou de domaines, des [noms d'hôtes par exemple]. Ils représentent des entités considérées comme malveillantes, indignes de confiance ou tout simplement ayant une mauvaise réputation.

Pour leur utilisation dans l'industrie ou dans la recherche, les gens les utilisent pour alimenter des pare-feu DNS afin d'empêcher le trafic malveillant de pénétrer dans leur réseau, typiquement le hameçonnage, ou de se connecter à des domaines ou des adresses IP malveillants. C'est surtout dans le cadre d'une réponse ou d'un incident à des fins d'application de la loi pour identifier les infrastructures malveillantes impliquées dans des attaques.

Il y a des exemples intéressants. Nous savons que les mécanismes de partage peuvent être commerciaux ou open source. Et ces listes peuvent être gérées par des entreprises commerciales, par exemple

Spamhaus, abuse.ch, Phish Tank, etc. Il y en a d'autres, la liste est longue.

Ces listes peuvent être spécifiques à la menace. Par exemple, nous avons abuse.ch qui a différentes utilisations, nous sommes pour tout ce qui est logiciels malveillants, hameçonnage, etc. et ils gèrent différentes menaces. Prochaine diapositive s'il vous plaît.

Nous en avons déjà parlé durant la section des panelistes. Nous avons des caractéristiques générales et des inconvénients. Je voudrais me focaliser sur les deux aspects. Pour quelqu'un qui fait de la recherche, les caractéristiques peuvent devenir des inconvénients.

Le point le plus important, c'est qu'on doit comprendre ce que l'on va faire et surtout ce que représentent les RBL et comment on peut les utiliser. Certaines de ces caractéristiques sont super spécialisées parce qu'elles ont un objectif spécifique. La personne qui veut les utiliser doit comprendre exactement à quoi elles servent.

En général – encore une fois, je parle selon ma position de chercheure –, il y a une couverture limitée et des points d'observation limités. Les personnes qui fournissent des données peuvent être moins bien représentées dans certains emplacements. Cela fait sept ou huit ans que nous étudions cela. La plupart du temps, les listes ont été améliorées quand il s'agit de la couverture, mais il est encore important de garder cela à l'esprit lorsque l'on discute de ce sujet.

Il y a aussi l'idée d'observer tout ce qui concerne la qualité et les différents paramètres de redevabilité. Tout cela n'est pas nouveau.

Dans cette présentation, il me manque certaines données académiques, mais vous pouvez bien sûr me contacter si vous en avez besoin.

Il y a aussi une autre question. Lorsqu'il s'agit des caractéristiques des RBL, il y a souvent un manque général de documentation sur les processus de collecte et de curation des données. Le problème avec les fournisseurs de listes, c'est que ce n'est pas un document simple. Cela pourrait être aussi plus détaillé, plus réactif, donc c'est difficile de maintenir cette liste pour qu'elle représente toutes les données que nous donnent les fournisseurs pour les flux d'alimentation spécifiques.

Bien sûr, il y a beaucoup de fournisseurs de RBL divers qui ont des méthodologies différentes. Cela mène à des impacts différents au niveau de la couverture et de l'efficacité du processus. Il ne s'agit pas d'une mauvaise chose parce que la diversité peut apporter plus d'informations sur la table, du moment que l'utilisateur comprennent de façon adéquate toutes ces données. Prochaine diapositive.

J'ai déjà parlé de cela. Pourquoi est-il important de connaître les inconvénients des ces caractéristiques dont on parlait ? C'est important pour tous les utilisateurs, que ce soit des opérateurs de réseau, des chercheurs, des entreprises de sécurité qui s'appuient sur ces ressources d'être mieux informés et de comprendre les inconvénient pour qu'ils puissent concevoir des défenses et des méthodes de curation plus efficaces qui tiennent en compte des forces et des limites complémentaires des listes de blocage individuelles lorsqu'elles sont utilisées de manière isolée ou en combinaison.

Il y a beaucoup d'exemples dans la communauté de l'ICANN. Nous disons souvent qu'il y a des ressources qui démontrent les tendances du hameçonnage. Comment on peut faire le contraste des certaines recherches faites par quelqu'un d'autre ? C'est ce que je voulais dire. Je pense que c'est le point principal de ma présentation : cela dépend de l'utilisation et de la chronologie, des processus qui sont utilisés. Les tendances peuvent donc dans ce sens être changées. À mon avis, suivant mon expérience, on peut se focaliser sur telle ou telle tendance. Bien sûr, c'est toujours du point de vue du flux d'alimentation des données. Ces listes sont toujours partielles. Point suivant s'il vous plaît.

Avec les diapositives suivantes, nous allons vous montrer comment nous utilisons les listes à l'ICANN. Vous avez donc l'utilisation que nous faisons par rapport au DAAR et beaucoup d'entre vous connaissent ce processus. Je ne voudrais pas entrer dans les détails, mais en résumé, le système prend les noms de domaine des opérateurs de registre, prend les noms de domaine à partir d'un flux d'alimentation présélectionné et peut ainsi contrôler. Cela chevauche les domaines à partir de la première ou de la secondes étape. Il y a des processus de calculs de taux journalier des domaines dans la zone qui apparaissent dans les RBL. Certains d'entre vous connaissent très bien le processus DAAR, soit le signalement des activités d'utilisation malveillante de domaine. Cela montre bien sûr les tendances, à savoir où les problèmes sont concentrés et bien sûr, cela va nous donner une idée à savoir si cette concentration change dans le temps. Bien sûr,

nous pouvons utiliser une certaine liste RBL en accordance avec nos projets. Prochaine diapositive.

BRENDA BREWER : Excusez-nous, on nous indique que vous devriez parler un petit peu plus lentement pour les interprètes.

SAMANEH TAJALIZADEHKHOOB : Parfait.

Nous avons aussi réalisé un projet au niveau des recherches pour le soutien à la conformité de l'ICANN et nous avons créé des indicateurs pour les bureaux d'enregistrement. C'était un projet au cours duquel nous avons fait quelque chose de similaire au DAAR et nous nous sommes focalisés sur le hameçonnage et les logiciels malveillants pendant une période d'un mois. Nous avons saisi une série d'indicateurs que nous avons présentés à un moment donné dans le temps. Et pour ce projet spécifique, nous avions accès au BRDA puisque nous ne pouvons utiliser que ce type de données au niveau de la conformité. Prochaine diapositive.

L'autre projet de recherche que nous faisons actuellement, nous utilisons les RBL pour mettre en place des modèles prédictifs de façon à pouvoir prédire la possibilité qu'un domaine devienne frauduleux et quelles sont les caractéristiques des domaines malveillants. Nous travaillons sur les mêmes méthodes que ce qui avait été fait dans le cas de l'étude COMAR qui a été déjà présentée lorsque nous avons eu des réunions lors des *Tech Day* à l'ICANN. Prochaine diapositive.

Comment nous évaluons ? Dans la plupart des projets que j'ai présentés dans la diapositive précédente, comment nous faisons des évaluations sur cette liste ? Nous avons un flux de réputation que nous contrôlons pendant une période de temps donnée et nous prenons les listes les plus réputées au sein de l'académie et du secteur en fonction des publications. Nous choisissons celles qui sont les mieux documentées et nous travaillons sur les listes qui existent en termes de couverture. Prochaine diapositive.

Cependant, nous sommes en train de planifier une évaluation plus vaste. C'est un travail en cours de réalisation.

Je voudrais aussi vous dire que le travail sur l'évaluation du RBL est quelque chose de long qui demande du temps. Ce que nous essayons ici, c'est de rendre notre travail le plus complet et le plus pertinent pour les personnes qui l'utilisent. Et nous travaillons sur l'élaboration d'indicateurs que nous appelons *Purity*, pureté, pour faire la différence entre les faux négatifs et les faux positifs.

Puisque nous avons des données sur le terrain que nous tirons, le premier problème concernant les RBL apparaît ici. Nous voulons aussi estimer la couverture, la capacité de réponse, l'exactitude, l'agilité, la stabilité dans le temps et le nombre de domaines qui sont vraiment de vrais positifs.

Ce que je viens de vous présenter, ce ne sont pas des choses qui sont terminées. Il peut y avoir des changements au fil du temps à mesure que nous travaillons sur ce projet de recherche. Et nous vous

tiendrons au courant. Pour le moment, c'est un travail qui est en cours de réalisation. Prochaine diapositive.

Ici, je vous donne les références que j'ai utilisées pour élaborer cette présentation.

J'en ai terminé avec ma présentation, mais je voudrais ajouter, puisqu'au niveau du responsable technique de l'ICANN nous avons plusieurs projets sur lesquels nous travaillons concernant les RBL pour les bureaux d'enregistrement et les opérateurs de registre, nous essayons de développer des indicateurs. Nous ne voulons pas publier des choses qui ne sont pas vraiment fiables, donc nous continuons à travailler sur cet aspect.

Par exemple, nous avons parlé du temps qui est nécessaire pour les opérateurs pour réagir en cas de menace contre leur sécurité. Pour en revenir un petit peu à la discussion qui avait lieu tout à l'heure concernant les différences de méthodologies qui existent, on constate que si on prend plusieurs listes et si on essaie de créer des indicateurs de performance pour des opérateurs concernant les réactions, on mélange différentes méthodologies et les indicateurs ne représentent plus rien de fiable vraiment. Donc tout dépend de la méthodologie utilisée par le fournisseur de RBL.

Donc ce sont des exemples réalisés par des personnes qui essaient de comprendre, qui essaient de voir quelles sont les données qui sont importantes à présenter pour les différents acteurs dans cette discussion.

Je vous remercie et je reste à votre disposition pour répondre à vos questions. Merci.

LG FORSBERG : Nous allons maintenant passer à la partie suivante de notre webinaire pour une question de temps. Donc nous allons entamer la deuxième partie.

La deuxième partie de ce séminaire va porter sur les conclusions. Je vais donner la parole aux parties contractantes et aux représentants de ce panel, à savoir Reg et Matt. Est-ce que vous utilisez des listes de réputation et de blocage aujourd'hui ? Et si c'est le cas, de quelle façon ? Nous allons d'abord donner la parole à Reg.

REG LEVY : Actuellement, nous n'utilisons pas de RBL, mais nous utilisons des rapports de manière régulière concernant ces RBL. La plupart des rapports ne nous donnent pas l'URL en question, donc il est difficile pour nous d'atténuer le problème parce que nous ne pouvons pas faire une différence entre ce qui est vraiment le problème, à savoir est-ce que c'est un domaine frauduleux, piraté ou est-ce que c'est un mauvais bureau d'enregistrement. Des fois, on peut prendre le domaine, regarder et dire : « OK, cela fait partie d'un système frauduleux. » D'autre fois, le domaine a déjà été retiré quand on arrive il n'est plus en ligne, donc c'est réglé.

Actuellement donc, nous ne voyons pas les différentes options qui sont à notre disposition. Ce qui est important pour nous, c'est la

rapidité de retrait de ces noms de domaine. À mon avis, cela ne suffit pas. Il ne suffit pas de rapporter le comportement d'un domaine, le rapport ne suffit pas. Nous devons aussi l'analyser et ensuite, nous le retirons de notre liste.

LG FORSBERG : Merci Reg.

Matthew, vous avez la parole.

MATT THOMAS : Je voudrais ajouter ici quelques points concernant l'utilisation des RBL et répondre à quelques questions.

Je dirais qu'il s'agit ici du contexte dont Carel a parlé et qui a été aussi mentionné par d'autres panelistes. Je crois qu'il est très important de comprendre le contexte dans lequel les RBL sont utilisées. Il faut dire que ce sont des outils très utiles s'ils sont utilisés correctement dans le contexte approprié.

Il faut comprendre pourquoi la RBL a été conçue. Ce sont des outils qui ont été conçus pour protéger les utilisateurs finaux, les environnements et les réseaux. Elles ont certaines priorités dans ce contexte qui vont répondre à leurs objectifs. Mais elles peuvent être parfois un peu conservatrices pour retirer certaines entrées.

Donc du point de vue de l'utilisateur en tant que praticien de la sécurité, je dirais qu'elles ont de bonnes propriétés dans le sens qu'on va être moins soucieux des faux positifs et plus soucieux de la

protection des utilisateurs finaux. Mais quand on commence à utiliser ces RBL dans d'autres contextes, il faut comprendre la priorité de ces RBL et comment elles vont avoir un impact sur la façon dont elles sont utilisées à travers différentes études et outils de mesure utilisés. Certaines RBL sont maintenues et cela va avoir une influence sur votre capacité à les utiliser de manière systématique.

Donc je dirais qu'il est important de faire attention à la façon dont ces RBL sont utilisées et appliquées.

LG FORSBERG : Merci Matt.

REG LEVY : Je dirais que la compréhension de la façon dont ces RBL sont construites est très importante pour les utiliser correctement aussi et pour utiliser leurs données.

LG FORSBERG : Merci beaucoup.

Est-ce que vous diriez que les parties contractantes, les bureaux d'enregistrement et les opérateurs de registre comptent sur l'aide des RBL et sur les données qui vous sont fournies ou est-ce que vous devez mettre à jour ces données ?

MATT THOMAS : C'est une question intéressante je dirais, LG. Et je pense qu'ici, ce qui m'intéresse, c'est le mot « plus ». Que signifie « plus » ? Comment on mesure « plus » ? Mesurer davantage dans le cas de l'utilisation malveillante des domaines ? Davantage de domaines sont retirés ? C'est ce que cela veut dire ou cela veut dire que ce sera plus efficace pour détruire l'infrastructure qui soutient les utilisations malveillantes qui existent sur le réseau ?

Je crois qu'il faut constater qu'il ne s'agit pas seulement des RBL et des parties contractantes qui sont en jeu dans cet écosystème ; c'est la communauté dans son ensemble qui doit se centrer sur les problèmes d'utilisation malveillante du DNS. Nous devons travailler tous ensemble pour rendre tout cela plus facile à mettre en œuvre. Nous devons travailler avec les fournisseurs d'hébergement, les forces de l'ordre, travailler tous ensemble pour commencer à combattre l'utilisation malveillante du DNS.

Je suis sûr que les fournisseurs de RBL ont des tas d'exemples de données qu'ils ont collectées, des domaines de hameçonnage qu'ils ont identifiés et qu'ils ont retirés et qui réapparaissent quelques heures plus tard. Donc ici, on a une question d'atténuation doit être faite davantage ou mieux. On peut se demander si l'utilisation malveillante en elle-même est paralysée, si elle est freinée. Je pense que nous devons travailler sur l'infrastructure, sur la partie systémique qui soutient tout cela.

Un autre exemple peut être un système comme Avalanche. On fait de gros efforts pour combattre ce type d'utilisation malveillante du DNS

parce que le problème sous-jacent est que la machine qui héberge ce système est modifiée et réadaptée à chaque fois.

Donc je crois qu'ici, nous avons la possibilité de répondre à votre question, LG, en disant qu'est-ce qui pourrait être fait dans le domaine des RBL au niveau des parties contractantes. Et je dirais qu'il faut se positionner correctement dans cet écosystème en fonction des observations faites, en fonction des données de façon, à savoir quel est le taux d'efficacité pour démanteler ce type de plateformes qui soutiennent l'utilisation malveillante des noms de domaine et du DNS. Je crois que nous pouvons travailler avec la communauté de l'ICANN pour mettre en œuvre cette réponse.

LG FORSBERG : Merci Matthew.

Reg, est-ce que vous avez une réponse ?

REG LEVY : Oui, je suis d'accord, comment essayer de définir ce qui est « plus » dans ce sens.

Nous travaillons régulièrement avec beaucoup de fournisseurs pour établir si on peut ou non utiliser leurs services pour atténuer les faux positifs. Les débats précédents indiquent qu'il y a un nombre de faux positifs et nous devons en comprendre le niveau, à quel niveau nous allons punir les titulaires de noms de domaine, savoir quand sont-ils coupables. Nous avons vraiment besoin de le définir.

LG FORSBERG : Merci Reg.

Je vais passer la parole à Joanna qui est la représentante des utilisateurs finaux à l'At-Large. Je voudrais lui demander ceci. De quelle manière est-ce que les fournisseurs de liste peuvent aider les utilisateurs qui ont eux-mêmes des problèmes avec ces listes de blocage et de réputation ?

JOANNA KULESZA : Je comprends qu'il y a des contraintes. Mais je voudrais en profiter pour participer à cela. C'est une bonne question pour la communauté At-Large. Nous aussi, nous essayons d'y répondre, à savoir comment ces listes RBL vont avoir une incidence sur les utilisateurs finaux. Quand est-ce qu'un nom de domaine se qualifie malveillant ? C'est un problème pour nous. Nous allons livrer ce message vers la communauté en général, mais nous représentons les utilisateurs. Nous sommes heureux de pouvoir participer à ce débat avec la chambre des parties contractantes, avec le GAC, etc.

Nous, normalement, les utilisateurs finaux, nous essayons de travailler avec les forces d'application de la loi et d'autres parties pour essayer d'obtenir assez de ressources et pouvoir fournir des services. Mais dans ce cas-là, si un utilisateur final suit le lien qui est sur une RBL, il va se retrouver avec un problème.

Donc il y a deux parties au problème. D'un côté, nous voulons avoir une réponse finale spécifique pour nos utilisateurs, comment ils

peuvent retirer un site web sur la liste qui est listé pour la mauvaise raison. Parce que bien sûr, il n'y a pas de liste générée. Donc nous voulons pouvoir discuter et pouvoir faire du renforcement des capacités dans ce sens avec nos utilisateurs pour nous assurer que les critères des listes noires reflètent les attentes.

Comme l'a dit Peter tout à l'heure, on veut savoir s'il y a un éléphant dans la pièce lorsqu'il s'agit de la redevabilité de la RBL. Nous avons vu durant le débat aujourd'hui qu'il y a des critères qui ont été pris en compte. Il y a eu des conversations entre ceux qui fournissent ces listes. Mais pour nous, pour que nous puissions bien comprendre comment fonctionne ce système, nous aurions besoin d'un dénominateur commun ou des opportunités comme celle-ci pour mieux comprendre comment ce système fonctionne et pouvoir continuer à contribuer à son développement.

Donc les critères qui seront utilisés pour mettre sur la liste noire certains sites web, c'est donc un débat qui va se dérouler au sein de la communauté ICANN et l'At-Large veut être entendue.

Nous avons organisé des webinaires, des séances, des discussions de politique interne pour essayer d'identifier la définition de l'utilisation malveillante du DNS. Nous avons essayé de répondre aux questions. Nous savons qu'il y a des questions de juridiction par exemple. Cette liste pour nous est un élément essentiel et nous avons besoin de savoir quels sont les critères utilisés. Nous sommes heureux de pouvoir participer à cette plénière pour pouvoir obtenir des réponses, à savoir comment les opérateurs de registre et les bureaux

d'enregistrement fonctionnent aussi dans ce sens. Pour moi, je pense que c'est vraiment un débat qui doit se poursuivre.

Merci.

LG FORSBERG : Merci Joanna.

Je voudrais faire écho avec une question pour les fournisseurs de RBL qui se rapporte à la déclaration que vient de faire Joanna. Comment est-ce que vous suggérez que les utilisateurs finaux qui ont été listés sur une des RBL puissent résoudre ce problème ? Comment vont-ils résoudre le fait qu'ils se trouvent sur une liste RBL ?

CAREL BITTER : Je ne sais pas ce que font les autres, mais je peux vous dire ce que nous faisons.

Nous avons un site web que vous pouvez consulter – puisque nous parlons des domaines – pour pouvoir être retiré de cette liste. Nous reconstruisons cet ensemble de données toutes les minutes.

Nous avons devoir créer une étiquette ou une sorte de document avec les paramètres que nous avons. Nous avons des personnes qui travaillent 24 heures sur 24 pour gérer tout cela et pour comprendre exactement quels sont les problèmes, ce qui doit être fait pour retirer ces domaines de la liste.

LG FORSBERG : Merci Carel.

Ben, vous pensez que c'est différent de ce que vous faites ?

BEN COON : C'est intéressant. Dans notre cas, la liste n'est utilisée qu'en segment de 24 heures. Nous faisons à peu près la même chose. Si quelqu'un signale un faux positif ou si quelqu'un rapporte quoi que ce soit vers nous qui n'est pas normal, nous allons étudier la chose en détail, à savoir pourquoi ce détail a été signalé et à savoir ce qui se produit vraiment derrière tout cela. Nous signalons tout cela vis-à-vis des bureaux d'enregistrement ou des fournisseurs d'hébergement. Ils reviennent vers nous et nous prenons les choses très sérieusement. Nous étudions cela vraiment de très près, à savoir ce que nous allons avancer comme informations, savoir si c'est vraiment du hameçonnage, si c'est vraiment malveillant. Nous le faisons dans les minutes à suivre.

LG FORSBERG : Merci Ben.

Il est clair qu'il n'y a pas un feedback générique qui soit en place pour signaler une indication d'utilisation malveillante ou un faux positif.

Roman, vous pensez que vous pourriez travailler sur une manière normalisée, standardisée pour pouvoir partager ces informations et recevoir toutes ces informations de sources diverses ? Et comment ce système pourrait être facilité et pourrait être fiable ?

ROMAN HUESSY : Je pense que c'est une question très intéressante. Je vais essayer de fournir une réponse.

Je pense que ce serait une bonne façon de générer de la confiance dans la communauté. C'est quelque chose qui pourrait être réalisé. Et vraiment, c'est une thématique de l'ICANN. C'est quelque chose qui doit être fait par l'ICANN.

LG FORSBERG : Merci Roman.

Joanna, je voudrais revenir vers vous et vous poser une autre question. Ce n'est pas seulement dirigé aux RBL, mais qu'est-ce qu'il nous faut pour nous assurer que les opérateurs de registre et les bureaux d'enregistrement n'agissent pas au-delà de leur mission quand il s'agit de l'utilisation malveillante du DNS ?

JOANNA KULESZA : Je voudrais faire écho à la déclaration de Matt. Il s'agit de la transparence. Le plus ouvert les fournisseurs de liste seront au début quand il s'agit des critères qui sont appliqués, plus ce sera facile pour l'utilisateur en général et pour qu'il puisse être entendu. Je pense vraiment que c'est là que l'At-Large peut aider pour identifier quelles sont les attentes.

La réponse pourrait être au niveau régional. Nous en avons parlé durant nos réunions. On a beaucoup travaillé sur l'utilisation

malveillante du DNS au niveau régional. Donc cette réponse pourrait venir du niveau régional. Les attentes peuvent être différentes d'un pays à l'autre, d'une région à l'autre. Nous savons exactement de quoi cela a l'air en Europe, mais cela pourrait être un avantage vis-à-vis du développement à l'avenir du modèle multipartite.

Il faut donc mettre le point sur la transparence de ces procédés et de la compréhension, à savoir comment tout cela fonctionne. Et je pense que tout cela va nous aider à avancer et à faire avancer ces listes RBL.

LG FORSBERG : Merci Joanna.

Je vais prendre une question. C'est une question qui vient d'un intervenant : « Pourquoi ces listes ne montrent pas de preuves dans les rapports ? Sans ces preuves, il est difficile d'agir. » Je vais passer cette question à Carel.

CAREL BITTER : Nous allons parler de l'aspect spam de ceci.

Nous recevons des rapports par exemple des entreprises, des FSI, de nos collaborateurs. Les spammers sont devenus très doués pour mettre en place des détails de suivi dans tout ce qu'ils font. L'échelle à laquelle nous recevons toutes ces choses rend les choses compliquées pour nous. Nous ne pouvons pas adresser tout cela et fournir des informations qui soient nettes et fournir des solutions qui soient claires. Et là, si on ne peut pas partager sans protéger ces sources,

alors on ne peut pas partager. Dans les cas individuels, nous voulons bien travailler avec les personnes et leur donner des informations qui sont partageables. Mais du côté automatisé, ce n'est pas vraiment évident de la faire.

Pour vous donner une idée, on reçoit à peu près 2 000 à 3 000 courriels par seconde. On ne pourrait absolument pas nous assurer que quelque chose est valable pour toutes ces informations et fournir les bonnes informations en retour et que toutes ces informations que nous recevons soient adéquates.

Comme je le disais, les gens qui font le travail d'atténuation ont besoin de preuves adéquates dans ce but. Pour cela, ils ont besoin d'obtenir plus de détails de la source pour faire leur travail.

LG FORSBERG : Merci Carel.

Nous arrivons à la fin de notre séance puisque nous n'avons pratiquement plus de temps. Quand on regarde les réponses au sondage que nous avons publié au départ de la séance, sachez qu'il y a beaucoup de personnes qui n'avaient jamais entendu parler de tous ces types d'utilisation malveillante et beaucoup bien sûr qui en avaient entendu parler. Il y a des personnes qui n'ont pas eu à subir ce genre d'utilisation malveillante et d'autres oui. Beaucoup d'entre nous bien sûr, j'espère que nous avons beaucoup appris de ce débat et que nous allons pouvoir partager ce message dans notre travail sur ce sujet particulier d'ailleurs.

Je voudrais remercier tous les panelistes pour leur temps, leur participation, le personnel de l'ICANN pour son support et surtout, toutes les personnes qui ont partagé ce temps avec nous durant cette semaine très occupée à l'ICANN.

Pour comprendre ces listes, leurs fonctions, leurs objectifs, comment nous les utilisons pour corriger les erreurs, c'est une étape importante pour combattre l'utilisation malveillante du DNS. Le parcours va être long.

Encore une fois, merci à tous d'avoir participé.

BRENDA BREWER : Il nous reste une question de sondage et nous allons la publier à l'écran d'un moment à l'autre. Merci de bien vouloir patienter.

Voilà, la question du sondage devrait être sur votre écran. Est-ce que vous savez comment signaler une menace de sécurité ou est-ce que vous connaissez les étapes pour signaler une menace ? Répondez par oui ou non. Encore une fois, la question est sur l'écran : est-ce que vous savez comment signaler une menace de sécurité ou est-ce que vous savez quelles sont les étapes que vous devez entreprendre pour atténuer cette menace ?

Merci. Et je vais présenter les résultats du sondage.

Merci à tous pour votre participation. Cette réunion est maintenant terminée.

[FIN DE LA TRANSCRIPTION]