SAN JUAN – Comment ça marche : comprendre l'utilisation malveillante du DNS
Lundi 12 mars 2018 – 13h30 à 15h00 AST
ICANN61 | San Juan, Porto Rico

CATHY PETERSEN : Bonjour à tous. Nous allons commencer d'ici peu cette séance sur comprendre l'utilisation malveillante du DNS. Merci.

Bonjour, bienvenue à cette séance consacrée à comprendre l'utilisation malveillante du DNS. Nous avons Carlos Alvarez du bureau du CTO qui va nous présenter ce sujet.

CARLOS ALVAREZ : Bonjour à tous. Merci à tous ceux qui sont ici dans la salle. Je sais qu'il y a 23 participants qui nous écoutent à distance ; bienvenue.

Nous allons parler d'un sujet qui est très important et qui peut donner lieu à des litiges. Et nous allons donc parler de l'utilisation malveillante du DNS.

Tout d'abord, nous allons essayer de voir quels sont les différents volets de cette discussion. Il y a donc différents volets pour comprendre quelles sont les perspectives pour comprendre l'abus du DNS ou l'utilisation malveillante du DNS. Nous allons parler de quelques exemples, nous allons parler

également du panorama changeant des menaces au DNS et nous allons parler également de l'utilisation malveillante du DNS dans le contexte de l'ICANN.

Premier point, il n'y a pas de définition globale et acceptée de ce que c'est que l'abus du DNS ou l'utilisation malveillante du DNS. Il y a certaines définitions qui varient et qui incluent d'autres sujets un peu plus larges tels que la cybercriminalité, le détournement de noms de domaine et les comportements malveillants.

Les menaces au DNS peuvent être regroupées en trois catégories : corruption de données, déni de service et atteinte à la confidentialité.

Il faut distinguer entre mauvaise utilisation du DNS et abus du DNS. Mauvaise utilisation fait référence à de comportements qui visent à tromper les utilisateurs. Et nous allons après nous pencher sur ce que c'est que l'utilisation malveillante du DNS.

Nous essayons donc de trouver, d'identifier des éléments pour savoir ce que c'est que l'abus du DNS, qu'est-ce que le GAC a dit par rapport à cette question qui est assez large. Le GAC dans son communiqué de Beijing a prévu des sauvegardes qui sont applicables aux nouveaux gTLD. Voilà ici un extrait de ce document, donc atténuation de l'activité abusive, distribution de logiciels malveillants, opérations de réseaux zombies,

hameçonnage, atteinte aux marques enregistrées, comportements frauduleux ou trompeurs. Cela semble assez vaste et certains considèrent que certains des éléments qui sont inclus dans cette définition ne sont pas liés à l'utilisation malveillante à proprement parler du DNS. Mais voilà un élément que nous avons pour penser à cette définition. Ensuite, nous avons les activités qui sont contraires aux lois applicables.

Il y a également une question qui reste ouverte en ce qui concerne le fait de savoir si le spam est ou devrait être considéré comme un cas d'abus du DNS dans le système des noms de domaine. Du côté de la communauté opérationnelle et du côté du renforcement de la loi, le spam serait un prédécesseur ou indicateur d'activité malveillante. En lui-même, le spam jusqu'à présent n'est pas considéré comme étant un abus du DNS du point de vue technique.

Alors quand vous faites des recherches au niveau des menaces et que vous analysez les données, vous voyez qu'il y a des campagnes de spam qui sont lancées, vous détectez quelles sont les infrastructures qui sont derrière le spam. Et si vous continuez à suivre leurs activités, tôt ou tard – en général, plus tôt que tard – vous voyez les activités de suivi qui s'appuient sur cette campagne de spam et qui peut consister à distribuer du matériel d'hameçonnage, matériel frauduleux, etc. Pour le dire tout simplement, l'abus du DNS fait référence à tout élément qui

va attaquer ou qui va utiliser à des fins malveillantes l'infrastructure du DNS.

Nous avons parlé de deux volets pour parler de cette question. D'un côté, il y a la perspective technique, c'est-à-dire la résolution des noms de domaine, comment ils se traduisent en adresse IP. Et l'autre perspective concerne les services d'enregistrement de noms de domaine. Ces services sont fournis par les bureaux d'enregistrement et par les opérateurs de registre et font l'objet d'utilisations malveillantes par des criminels. En ce qui concerne la mauvaise utilisation du DNS, cela fait référence au fait d'exploiter les protocoles de DNS ou les processus d'enregistrement de nom de domaine à des fins malveillantes. Très bien.

Ce n'est pas nécessaire de lire cette diapositive. L'idée de cette diapositive, c'est de vous montrer quels sont les éléments opérationnels du DNS de manière simplifiée. Nous avons dans la première case bleue les serveurs de noms qui font autorité ; il y a un serveur pour chaque domaine. Ensuite, vous avez les serveurs de noms récursifs que l'on peut considérer comme les serveurs du DNS que le fournisseur d'accès internet va interroger pour pouvoir résoudre leur nom. Et ensuite, nous avons le client ou les résolveurs finaux et qui fonctionne, par exemple dans nom navigateur, il va chercher donc l'information dont j'ai besoin pour pouvoir résoudre un nom de domaine. Si je

vais par exemple à www.icann.org, le résolveur minimum va essayer de résoudre cette adresse, va trouver où se trouve hébergé le contenu du site www.icann.org et va essayer d'obtenir ces informations.

Ce sont les trois éléments opérationnels du DNS et ces trois éléments peuvent devenir des cibles pour les attaquants.

Voyons maintenant les attaques par réflexion, par amplification qui vont attaquer le cœur même du DNS en distribuant du matériel malveillant.

Qu'est-ce que c'est qu'une attaque par réflexion ? Cela veut dire que vous pouvez envoyer un paquet qui falsifie des informations sur l'adresse IP source. Donc le serveur croit que ce paquet a été envoyé par quelqu'un d'autre. Ce serveur va envoyer donc une réponse à cette autre adresse IP qui est falsifiée. Donc par exemple je vais envoyer un paquet à Cathy mais finalement, le paquet arrive au serveur DNS et l'adresse IP de ce paquet dira que ce paquet vient de Cathy et non pas de moi. Si je fais cela et que j'utilise ce que l'on dit, les résolveurs ouverts – c'est des résolveurs qui existent, il y en a des centaines – et qui ne filtrent pas les adresses IP par rapport à leur provenance, alors Cathy aura énormément de requêtes. Je vais envoyer des requêtes DNS à des centaines de ces résolveurs ouverts qui se trouvent

dans le DNS et toutes ces requêtes vont venir vers Cathy. Et c'est ce que l'on appelle une attaque par réflexion.

Une autre attaque, c'est l'attaque par amplification. Que veut dire cela ? C'est-à-dire que chaque interrogation ou chaque requête est petite et en général, c'est une ligne de code. Et cette ligne peut dire par exemple dig nom de serveur, nom de domaine any. Ça y est et c'est parti. Ce sont sept octets, c'est vraiment petit, c'est juste une ligne de code. Alors que la réponse sera très longue. Elle peut faire 2,5 mégabytes par exemple, multipliez cela par les centaines de requêtes que mon réseau zombie envoie. Vous vous souvenez, un réseau zombie, c'est un réseau avec beaucoup d'ordinateurs qui vont envoyer des requêtes, des ordis qui sont compromis. Les criminels qui opèrent ces réseaux zombie peuvent compromettre énormément d'ordinateurs qui vont envoyer à leur tour toutes ces requêtes. Et ces requêtes auront leur réponse et ces réponses seront envoyées à Cathy.

Donc je vais utiliser ces centaines de résolveurs ouverts pour leur envoyer ces petites lignes de code qui vont produire des énormes réponses. Et la façon dont ils écrivent la ligne de code qui est envoyée est telle que la réponse est très longue. Et ces réponses vont arriver à Cathy. Et Cathy, si elle ne peut pas contrôler ce trafic qui va venir vers elle, elle sera victime de cette attaque par amplification.

En 2003, le DNS a été utilisé comme vecteur d'attaque par Spamhaus. Ce sont des données intéressantes que l'on peut tirer de cette attaque pour essayer d'atténuer ce type de risque. Bien sûr, le DNS n'est pas le seul vecteur d'attaque mais en tant que protocole, il peut être exploité à des fins malveillantes. Nous allons parler également d'empoisonnement de cache et aussi de l'attaque de l'homme du milieu. Ce sont des attaques également qui utilisent le DNS comme vecteur. Très bien.

Vous voyez ici ce que je viens de vous décrire. C'est une attaque large qui utilise la réflexion, c'est-à-dire on envoie des paquets qui ont une adresse IP falsifiée. Ces adresses sont lues par les résolveurs ouverts qui pensent que Cathy envoie ces requêtes. Ensuite, ces requêtes qu'ils reçoivent déclenchent une réponse très large ; c'est la réponse par amplification. Et à ce moment, Cathy est inondée de requêtes. C'est exactement ce que je viens de vous décrire.

Ce n'était pas moi qui ait fait défilé toutes les diapositives. J'ai pris trop de café je pense, cela va trop vite. Nous étions là, d'accord.

Une autre forme d'attaque du DNS consiste à s'attaquer aux serveurs de noms. Cela fait partie des résolutions de noms de domaine. Par exemple, si j'ai mon nom Carlos, je dois configurer deux serveurs. Le DNS est un système global qui a des

ressources associées à mon nom. Autrement dit, je dois définir et rendre ces informations disponibles aux différents serveurs. Et pour le dire très simplement, par exemple ces serveurs doivent savoir où se trouve mon serveur de messagerie, mon serveur de nom, etc. Donc si quelqu'un veut interroger ces serveurs et que ces serveurs ne sont pas disponibles, personne ne pourra obtenir les réponses associées à mon nom de domaine et mon site web ne sera pas disponible.

Ce type d'attaque est utilisé par les criminels pour exploiter à des fins malveillantes le protocole TCP. Quand on envoie un paquet TCP au serveur, le serveur répond à cette connexion TCP. À ce moment-là, autant le dispositif qui lance la connexion et l'autre dispositif créent une connexion. Cela veut dire que tous ces deux dispositifs doivent allouer certaines ressources pour pouvoir maintenir connecté ce canal de communication. Et c'est comme cela qu'on peut compromettre des ordinateurs dans un réseau zombie. On peut envoyer des requêtes à un serveur de noms de telle sorte que ce serveur est forcé à établir trop de connexions TCP, c'est-à-dire qu'il doit allouer des ressources pour pouvoir maintenir ces connexions en fonctionnement. Et à ce moment-là, on arrive à un point où ce serveur ne pourra plus avoir de ressources disponibles pour établir d'autres connexions TCP. Et cela veut dire que personne d'autre ne pourra interroger ce serveur pour obtenir des informations. Le serveur sera

toujours en ligne mais il ne sera pas en mesure de répondre à des requêtes. C'est ce que l'on dit dans cette diapositive. Si vous avez de la chance, vous pouvez obtenir une réponse quelques minutes après. Mais si vous multipliez cela par le nombre de trafic qui existe dans le nom de domaine, vous pouvez perdre absolument la possibilité de résoudre des noms de domaine.

Empoisonnement d'un cache : il s'agit des criminels quand ils veulent être créatifs. Parfois, ils ne le sont pas tellement. Vous vous souvenez que nous avons parlé dans une diapositive précédente qu'au sommet, nous avons le serveur faisant autorité, par exemple si je veux créer un site web et je veux associer dns.carlos.quelquechose pour fournir au DNS des informations associées à mon service de messagerie, mon service web, etc. Ce sont mes serveurs de noms qui font autorités.

Mais après, tous les FSI, fournisseurs de service internet, et tous les autres acteurs du DNS, tous les fournisseurs de service internet, ce sont des serveurs récursifs. Cela veut dire qu'ils posent des questions, ils interrogent d'autres serveurs à la place de quelqu'un d'autre. Et il y a certains de ces résolveurs récursifs qui ne sont pas bien protégés et qui sont vulnérables. Imaginez par exemple des centaines de fournisseurs internet qui sont là dans différentes régions. Certains d'entre eux sont des petites sociétés qui n'ont pas beaucoup de ressources. Ils ont

l'infrastructure pour fonctionner mais ils n'ont peut-être pas les ressources pour protéger ces infrastructures. Et quand les serveurs ne sont pas suffisamment protégés, les criminels peuvent les compromettre de différentes façons.

Une de ces façons consiste à faire en sorte que si moi, je suis un utilisateur et que le fournisseur de service internet a un de ses résolveurs qui est compromis, une fois que j'envoie une requête, que j'interroge ce serveur par exemple pour trouver un .com, je veux obtenir une réponse correcte. Mais si le résolveur est compromis, les criminels peuvent ajouter un bout d'information supplémentaire et ce bout d'information complémentaire va me dire : « Ah, l'information que vous cherchez est celle-ci. » Et automatiquement, mes dispositifs vont mettre à jour les informations qu'il possède avec ces informations. Et ces informations ne sont pas valables. Et quand cela se passe, la prochaine fois que je vais vouloir accéder à ce site web, par exemple bankofamerica, je serai redirigé vers le site que les criminels veulent que je visite.

Et qu'est-ce qui se passe à ce moment-là ? Je vais donc visiter le serveur des criminels, je vais voir le contenu qu'ils veulent que je vois, cela peut être un site par exemple d'hameçonnage qui se fait passer pour le site bankofamerica. Et ils vont me demander mon mot de passe par exemple. Ils peuvent à ce moment-là voler mon mot de passe pour entrer dans mon compte du

bankofamerica. Et donc votre dispositif peut être compromis directement et ils peuvent modifier la configuration du DNS.

Je vous ai montré l'exemple des réseaux zombies. Il y a eu quelques années, quatre ans je crois, on a démantelé un réseau zombie. Par exemple, si mon dispositif est configuré pour envoyer des requêtes DNS à trois, quatre points et qu'il change l'adresse IP dans mon dispositif ou dans mon ordinateur, et au lieu d'avoir cette adresse IP, la mienne, une adresse IP qui n'est pas la mienne et qui est configurée pour fournir d'autres adresses IP vers leur propre infrastructure, ils auront tous les utilisateurs qui ont des dispositifs compromis, tous ces utilisateurs vont visiter leurs sites web, les sites web criminels. Nous allons en reparler plus tard.

Dans des cas comme celui-ci, lorsqu'on parle d'empoisonnement de cache, ce qu'ils font, c'est qu'ils compromettent les dispositifs des utilisateurs, ils envoient des requêtes au serveur DNS. Et admettons que je veux accéder à un nouveau site news.quelquechose, mais c'est un site qui n'est pas pertinent pour les criminels. Comme ils ont fait dans l'exemple précédent, ils vont ajouter un bout d'information à la réponse que leur serveur envoie à mon dispositif. Et ce bout d'informations supplémentaires pourrait être « Ah oui, l'adresse IP du site de votre banque est celle-ci. » Et encore une fois, dans

une période de temps défini, ma requête pour connaître le nom de domaine de ma banque finit dans le site web des criminels.

Donc ce type de changement de DNS est justement le type de logiciels malveillants dont je parlais, c'est-à-dire que la configuration de DNS qui a été conçue pour l'utilisateur a été changée. Et c'est présent partout, c'est-à-dire que les personnes qui dirigeaient ce réseau zombie, les personnes qui ont créé ce type d'attaque ont gagné beaucoup d'argent avant que les opérations d'application de la loi n'aient été mises en place. À ce moment-là, les forces de l'ordre ont pu utiliser des preuves qui disaient que ces personnes avaient gagné 25 millions d'euros, ce qui ne veut pas dire qu'ils n'ont pas gagné plus que cela. Mais on avait des preuves qu'ils avaient touché 25 millions de dollars, justement.

Avec ce DNSChanger, on peut changer la configuration dans tous les dispositifs des utilisateurs. Et ils faisaient quelque chose qui ne semblait pas être nocif, dans le sens qu'ils changeaient les publicités auxquelles accédaient les personnes sur les sites web. C'est-à-dire que lorsque j'accédais à mon site web préféré pour lire les nouvelles le matin dans mon bureau, au lieu de voir les publicités légitimes que j'aurais dû voir, ils les remplaçaient par leurs propres publicités. Et cela se faisait de manière permanente et cela a eu lieu pendant très longtemps. Donc vous voyez que cela leur a fait gagné beaucoup d'argent. On ne dirait

pas que c'est nocif mais ce l'est en réalité. Donc pour les utilisateurs, ils ne voyaient pas comportements étranges, ils avaient toujours les contenus auxquels ils voulaient accéder, ils pouvaient toujours interagir avec l'internet, avec les ressources dont ils avaient besoin. Donc apparemment, rien d'étrange n'avait lieu alors qu'en fait, c'était le cas.

Alors on a pris des mesures et il y avait tellement de dispositifs qui avaient été infectés, je ne sais pas combien mais c'était dans les centaines de milliers de dispositifs qui avaient été attaqués par ce type de logiciel malveillant dans beaucoup de pays. Je n'en suis pas sûr mais je pense qu'on en était dans la vingtaine de pays.

Lorsque les forces de l'ordre se sont impliquées, ils ont vu qu'il allait falloir qu'ils fassent quelque chose avec ces serveurs de noms que les délinquants ont exploités. Ils auraient dû les éteindre ; d'une part, c'était une possibilité. Mais si tous les dispositifs envoyaient des requêtes à ces serveurs, quel aurait été le résultat à votre avis ? Les utilisateurs auraient crû qu'ils n'auraient plus d'accès à internet. Ils seraient toujours connectés à internet mais leur dispositif n'aurait pas pu résoudre les noms parce que les résolveurs, les serveurs de DNS étaient éteints. Donc ils ne pouvaient pas tout simplement les éteindre. Ce qu'ils ont fait était d'utiliser les services d'ingénierie pour remplacer ces serveurs. Et les tribunaux ont assigné des

administrateurs pour ces serveurs pendant une période au cours de laquelle les différentes campagnes de lutte contre ce problème ont été mises en place dans les différentes juridictions pour que les utilisateurs se rendent compte qu'il allait falloir qu'ils fassent un nettoyage sur leur dispositif.

Bien sûr, étant donné que ces personnes étaient des délinquants, ils étaient aussi ingénieux. Donc ils ont trouvé différentes manières pour utiliser de manière malveillante les protocoles de DNS. Et au moins du point de vue académique, certaines de ces formes sont intéressantes. Cela montre une certaine créativité à des fins malveillantes, certes, mais c'est très créatif en tout cas.

Donc le protocole DNS était utilisé pour créer un canal caché d'exfiltration de données, ce qui a lieu lorsqu'on peut cacher des données sans que l'administrateur du réseau se rende compte que ces données sont volées. Voilà la partie qui a été cachée. Et le DNS, comme vous savez est considéré comme un canal caché d'exfiltration de données parce que ce port qui est utilisé pour les communications du DNS n'est pas bloqué ; on ne peut pas le bloquer. C'est-à-dire que le trafic dans les réseaux voyage d'un port à un autre. On passe toujours par des ports. Le port qui est utilisé par le DNS est le port 53. Et bien qu'il y ait des manières à travers lesquelles les ingénieurs peuvent réassigner ce port à l'interne dans leur propre réseau, cela comporte certaines

complications. Donc on ne le change pas souvent ou on ne le change pas jamais parce que c'est compliqué, c'est-à-dire que le port 53 ne peut pas être bloqué ou c'est très compliqué que de le bloquer parce que c'est très compliqué de le réassigner. Si ce port était bloqué, les personnes n'auraient plus de résolution de DNS, cela veut dire qu'elles penseraient que tout va bien, qu'ils sont déconnectés.

Donc en fait, on a deux manières d'utiliser le protocole DNS comme un canal caché d'exfiltration de données. D'une part, on attaque le dispositif et on le fait envoyer des requêtes DNS lentement à un serveur de nom délinquant. Mais dans chaque requête DNS, les délinquants auront remplacé les parties les moins importantes avec des bits qui correspondent aux données qu'ils sont en train d'exfiltrer. Donc les requêtes de DNS sont toujours des requêtes DNS. Si l'équipe d'ingénierie ou si l'administrateur du réseau vérifie ces requêtes et qu'il regarde le trafic, ce sera toujours des requêtes DNS. Mais il faudrait qu'il fasse un recueil de toutes les requêtes DNS qu'ils sont en train d'utiliser pour l'exfiltration de ces données. Et en fait, cela requiert une certaine analyse que de se rendre compte que ces requêtes ont été modifiées. Il faut voir tous ces petits bouts pour se rendre compte que ces données sont en train d'être exfiltrées.

Et puis les délinquants ont utilisé également le DNS pour exfiltrer des données à travers le texte. Lorsqu'on crée un nom

de DNS, il faut gérer, exploiter un fichier de zone. Dans le fichier de zone, on définit les ressources qui sont associées à ce fichier, c'est-à-dire qu'on comprend les informations du site web, du serveur de mail, de serveur FTP, s'il vous faut une signature DNNSEC, ces informations y seront contenues, si vous avez des informations de protection pour vos clients. Peut-être que vous aurez entendu parler de tout cela. Ce sont plus des sigles qui semblent protéger les utilisateurs en fait, en quelques mots

Tous ces types d'informations sont inclus dans les registres de texte et on peut ajouter n'importe quelle information à ces registres de texte. Il n'y a pas de limitation au type de texte qui peut être contenu dans ces types de recherches et de registres ; c'est du texte. Et les délinquants utilisent donc ces registres de texte pour exfiltrer des informations également. Ils peuvent utiliser des informations de requêtes dans ces textes à un serveur de noms qui va consolider ces informations, les regrouper et recréer les données qui ont été exfiltrées.

Et puis on a le fast flux, le flux rapide. Je pense que cela est abordé un peu plus tard. Sinon, on reviendra dessus.

Les enregistrements des noms de domaine sont en fait des sites faciles pour les attaques ; cela est évident. Les délinquants agissent à des fins malveillantes et malheureusement les services d'enregistrement des gTLD et des ccTLD sont donc les

moyens qu'ils utilisent. Ils veulent utiliser de manière malveillante les revendeurs, ils veulent utiliser des noms de domaine qui sont [inintelligible]. C'est un problème très difficile à résoudre. Les prix plus abordables de noms de domaine ont tendance à attirer les mauvais acteurs, ce qui fait partie de la nature humaine, je suppose. Si c'est moins cher, c'est mieux. Donc ils vont chercher plus de noms de domaine pour essayer de faire ces attaques. Les titulaires de noms de domaine et les utilisateurs sont en fait attirés par ces noms de domaine qui sont moins chers. C'est dans notre essence en tant qu'être humain comme je disais.

Et puis l'enregistrement des noms de domaine a évolué parce que l'industrie a évolué. Donc maintenant, on peut exploiter de grands portefeuilles de noms de domaine et les délinquants vont être là à les utiliser à des fins malveillantes, bien sûr. Donc on a des noms de domaine de DGA, c'est-à-dire l'automatisation dans les mains de ces délinquants pour la création et l'enregistrement de ces noms de domaine.

DGA, c'est quoi ? C'est l'algorithme de génération de domaine. C'est le sigle en anglais, DGA. Si vous imaginez un réseau zombie, il faut qu'ils aient tous leur propre infrastructure de contrôle et de commande qui est utilisée pour justement contrôler et gérer leurs infrastructures.

Mais qu'en est-il si cette infrastructure est éliminée ? Il leur faut un plan B, C, D, E, F, G, etc. Et c'est pour cela qu'on a les DGA. Lorsque les réseaux zombie se rendent compte qu'une des parties de ces réseaux associés à l'attaque command-and-control ne fonctionne pas, cela va signaler ce problème. Il y a énormément de problèmes et d'exemples de ce comportement de DGA. Je n'en ai donné qu'un exemple. Mais cela va envoyer un message que les fonctions de commande et contrôle de réseaux zombie ne fonctionnent pas. Cela montre que les fonctions de commande et contrôle du réseau zombie ont diminué parce qu'on a pris les mesures d'action. Et donc l'atténuation de ce problème va générer une signalisation qui leur fera savoir qu'il faut qu'ils redoublent leurs efforts pour continuer leurs opérations.

J'espère qu'on en sera presqu'à mon exemple.

Pourquoi les attaquants et les délinquants enregistrent-ils des noms de domaine ? Pour faire n'importe quoi : pour le hameçonnage, pour le rançongiciel, pour les sites des distribution de logiciels malveillants, pour ce que vous voulez en fait.

Et puis dans cette dernière ligne, on a l'administration des fonctions de commande et contrôle des réseaux zombies qui fournit la stabilité et qui attaque la résilience du DNS. C'est cela

qui nous inquiète le plus, que cela attaque la stabilisé et la résilience.

Des fois, on se demande par rapport aux sites pharmaceutiques illégitimes, et on se demande des fois si cela devrait être considérés dans les cas d'utilisations malveillantes du DNS ou pas. C'est plutôt similaire aux sites web de ventes de contrefaçons. Et c'est vrai mais des fois, il faut aller au-delà de la surface. Je ne peux pas expliquer tous les détails mais sachez qu'il y a d'autres niveaux de complexité au-delà de la surface. Vous croirez peut-être que ce sont quelques sites web qui sont utilisés pour vendre des médicaments de manière illégale dans certaines juridictions mais en fait, c'est bien plus que cela. Et c'est quelque chose de très offensif pour beaucoup de personnes.

Vous avez une question ? Oui, rapprochez-vous du micro s'il vous plaît.

CATHY PETERSEN : Sentez-vous libre d'utiliser les microphones qui sont à table. Dites vos noms et vos affiliations, s'il y en avait.

FARZANEH BADII : Bonjour. Je suis la présidente de la NCSG et j'ai une question à vous poser en mon propre nom personnel. Lorsque vous parlez

des noms de domaine qui vendent des produits pharmaceutiques de manière illégale et qu'il se pourrait qu'il y ait d'autres aspects négatifs, vous parlez de l'utilisation malveillante au niveau technique ou de la vente des contenus ?

CARLOS ALVAREZ : Je parle des opérations délinquantes qui utilisent des noms de domaine. Donc c'est l'utilisation des noms de domaine par rapport au contenu du site web et à l'activité délinquante, l'activité illégale qui suite.

FARZANEH BADII : En fait, cela n'a rien à voir avec le DNS les opérations de...

CARLOS ALVAREZ : Oui, c'est l'utilisation du nom de domaine, exactement, oui. Bien sûr.

Alors pourquoi payer si on peut tout simplement le saisir ? Pourquoi les délinquants payeraient-ils pour des noms de domaine ou pourquoi choisiraient-ils de payer s'ils peuvent tout simplement les prendre et obtenir le contrôle d'un nom pour lequel quelqu'un a payé ? Dans certaines situations, les délinquants choisiraient de détourner les noms de domaine plutôt que de payer pour ces noms. Donc ils peuvent attaquer

l'utilisation de ces informations d'accès des titulaires des noms de domaine pour accéder à leur panel de contrôle qui permet aux titulaires de gérer leur nom de domaine. Donc imaginez une organisation délinquante qui voudrait saisir un nom de domaine de grande valeur ou qui voudrait peut-être attaquer les clients d'une banque spécifique. Il pourrait très bien envoyer une campagne d'hameçonnage qui cible les utilisateurs qui sont des clients de cette banque, peut-être attirer les travailleurs de cette banque pour qu'ils fassent clic sur un lien sur lequel ils ne devraient pas avoir cliqué et puis leur voler leurs informations d'accès. Et puis une fois qu'ils ont ces informations, ils peuvent faire tout ce qu'ils veulent, ces délinquants. Ils peuvent simplement créer un nom de domaine de troisième niveau au-dessous du nom de domaine de second niveau, c'est-à-dire que si ma banque est la banque carlos.nimportequoi, le délinquant pourrait créer Ilphishyou.carlos.nimportequoi. Et donc à ce moment-là, ils pourraient envoyer des courriels avec cette adresse, ce qui attirerait les personnes avec plus de succès parce que les personnes verraient qu'il y a le vrai nom de domaine de ma banque dans ce mail. Ou alors, ils changeraient complètement les serveurs de noms et ils changeraient toutes les informations associées à ce nom de domaine. Donc ils pourraient changer tous les registres, ils pourraient tout simplement éliminer, supprimer toutes les informations de ma banque telles qu'elles apparaissent dans la zone racine.

Et puis il y a d'autres situations dans lesquelles les titulaires des noms de domaine qui n'avaient pas de bonnes mesures de sécurité pour leur infrastructure ont été attaqués. Ce n'est pas souvent, ce qui est suffisamment bien mais cela arrive et si cela arrive, ce n'est pas bon, surtout dans les cas où nous voyons que les délinquants ont ciblé des cibles de grande valeur et les titulaires ont répondu très rapidement – il y a un certain temps de cela – et heureusement, cela a été très bien abordé. Mais les délinquants auraient pu faire n'importe quoi s'ils avaient pu contrôler ces serveurs. Donc on voit qu'il y a des attaques du côté de l'utilisateur si les titulaires sont attirés à cliquer sur un courriel frauduleux ou alors on pourrait avoir des attaques sur l'infrastructure d'enregistrement si ces délinquants réussissent.

Voilà ce dont je parlais. Ici, on a un autre aspect ou une autre méthodologie d'hameçonnage. Les titulaires auraient les mêmes informations d'accès au panel de contrôle à travers lequel ils gèrent leur nom de domaine. Mais combien de titulaires auraient-ils leurs mêmes informations dans ce panel de contrôle que dans un autre compte qui avait déjà été attaqué ? En fait, dans la plupart des attaques que nous voyons chaque semaine ou chaque mois, on a toujours les mêmes informations. Et en fait, les délinquants essaient d'accéder à autant de services que possible avec des paires de noms d'utilisateur et mots de passe qu'ils ont attaqué dans d'autres

vols d'informations. C'est-à-dire qu'une fois qu'ils ont un mot de passe et un utilisateur, ils peuvent l'utiliser pour tous vos noms de domaine. Donc une fois qu'ils auront pris les informations pour un nom de domaine, ils ont tout attaqué. Il y a énormément de personnes qui utilisent les mêmes informations pour accéder à tous leurs comptes. Donc il faut conscients de cela.

Voilà fast flux. Il s'agit d'une technique que les délinquants utilisent pour pouvoir passer d'une adresse IP à une autre très rapidement, ce qui devient de plus en plus compliqué pour les forces de l'ordre et pour l'atténuation de ces attaques. Tout cela est défini dans les fichiers de zone, ce qui montre le TTL. Cela change le TTL, c'est-à-dire le temps à vivre, c'est-à-dire le temps de validité de cette réponse au cours de ce temps. La requête associée à un nom de domaine a une adresse IP. Une fois que ce délai sera passé, il faudrait renvoyer la requête pour obtenir ces informations. Et à ce moment-là, les serveurs donneront une adresse IP différente en réponse, c'est-à-dire que lorsque vous voyez TTL 120 secondes, deux ou trois minutes 180 secondes, les services d'annuaire vont se méfier de cela en fait.

Ici, pourtant, il faut savoir que les CDN, ce sont les réseaux de contenu d'adressage, donc ils fournissent des services qui permettent d'avoir un service équilibré, résilient, etc. qui utilise également des durées plus courtes pour ces TTL. Mais les

systèmes savent faire la distinction entre les deux. Or, si vous trouvez un nom de domaine qui a un TTL très court et qui est associé à une infrastructure récente qui pourrait être associée à un spam par exemple, cela va immédiatement signaler ou mettre en garde le système. Donc les chercheurs en fait sont plutôt tentés de bloquer ce système pour l'infrastructure. Pardon, c'était moi.

Le double fast flux. Que se passe-t-il dans ce cas ? Lorsqu'on peut identifier une opération criminelle où les pirates utilisent le double fast flux, on voit que le contenu est dans un serveur dans un pays. Deux minutes après, ce contenu n'est plus dans ce serveur, il set passé dans un autre serveur. Deux minutes après, ce contenu passe dans un autre serveur dans un autre pays et deux minutes après, le contenu bascule dans un autre serveur, dans un quatrième ou cinquième pays. Et ainsi de suite.

Comment les forces de l'ordre peuvent résoudre ce problème ? C'est très difficile. Le double fast flux que vous voyez ici, c'est une technique que l'on a pu voir dans un énorme service de nuage pirate qu'est s'est appelé Avalanche. Les pirates se sont servis de cette technique de double fast flux et ce qu'ils faisaient, c'était changer les noms très souvent. Donc si je voulais par exemple interroger carlos.jenesaispasquoi, si j'interroge le serveur dans deux minutes, j'obtiens une réponse. Deux minutes après, la réponse est différente. Et à chaque

requête, la réponse sera différente et les noms de serveur changeaient également leur adresse IP à chaque fois. C'est deux fois plus compliqué, deux fois plus embêtant et deux fois plus difficile à identifier. Heureusement, les pirates d'Avalanche ont été identifiés et ils sont derrière les barreaux.

Je vous ai parlé du DNS comme un canal caché d'exfiltration de données. Et le DNS est utilisé non seulement pour exfiltrer des données mais aussi pour infecter ou compromettre les dispositifs. Alors à travers le DNS, les criminels fournissent des instructions aux dispositifs. Les criminels peuvent injecter du logiciel malveillant dans le DNS et c'est vraiment très compliqué, comme je vous l'ai dit.

Le port 53 qui est utilisé pour les communications internet ne peut pas être bloqué et il faut mettre en place des techniques pour identifier ce type de problème. Il y a des techniques auxquelles je ne vais pas faire référence en ce moment, mais c'est à chaque opérateur de réseau de mettre en place de type de technique.

Nous avons vu cela également, deux exemples de criminels qui utilisent donc le DNS comme un canal caché. Vous voyez ici un réseau zombie qui envoie des réponses qui sont envoyées au serveur de noms. Et les criminels ont configuré ce serveur DNS pour fournir une réponse sous forme... c'est-à-dire

l'interrogation, la requête visait un enregistrement de texte et la réponse est une réponse qui est déjà compromise. Ces instructions peuvent attaquer cette cible, vous pouvez trouver tout type d'instructions.

Le panorama des menaces du DNS évolue. Les attaques par déni de service comme un service. Est-ce que vous vous souvenez de ce type d'attaque ? Mirai, vous vous souvenez de l'attaque Mirai ? Comment je pourrais expliquer cette attaque ? Il y a une association entre les fournisseurs de ce que l'on appelle stresser services qui ont été attaqués par ces réseaux zombie. Et donc il s'agit d'un site web qu'un enfant a créé quelque part. Et ce qu'ils disent, c'est que ce site vend des capacités pour que vous puissiez tester la stabilité de vos serveurs. Donc vous payez de l'argent et ce qu'ils font, ils disent qu'ils vous fournissent un certain nombre de trafic pour que vous puissiez tester votre infrastructure pour voir si votre infrastructure est résiliente et si elle peut supporter une attaque.

Le problème, c'est que ces services peuvent vendre ce service à n'importe qui. Autrement dit, ce sont des services de DDoS que l'on peut quelque part louer pour faire des attaques. On peut entrer en ligne, chercher un site, retrouver ce type de service. Il y en a, même, qui acceptent un paiement par carte de crédit, ce qui rend les choses un peu plus faciles pour les forces de l'ordre.

Mais tout ce que vous devez faire, c'est de payer et fournir l'information de la cible que vous voulez tester parce que bien sûr, on veut s'assurer que c'est un réseau résilient, tu vois ? Et ils font cela à travers différents moyens. Un de ces moyens, c'est les botnets ou les réseaux zombie opérationnels. On en déjà parlé, on a parlé de fast flux, double fast flux. On a parlé d'Avalanche également. Nous allons parler plus tard [inintelligible]; c'était aussi une affaire assez compliquée.

L'internet des objets. Je n'en ai pas parlé de cela mais on sait qu'il y a une menace aussi dans l'internet de objets. Un bon exemple de cela est des systèmes vulnérables. Un bon exemple de cela, je pense que c'était en octobre ou septembre 2016, il y a eu une attaque à OVH. C'est un fournisseur d'accès de France. Dans cette attaque, les criminels ont pu détecter que l'attaque venait de plus de 1000 caméras numériques. Le réseau zombie avait la capacité d'envoyer 1,5 térabytes de données. C'était énorme, c'était quelque chose de jamais vu à l'époque ; je ne peux même pas l'imaginer. Mais ils ont pu mesurer 1,5 térabytes comme trafic dirigé vers ce fournisseur. Et c'était des caméras vidéo. Ce n'est pas nouveau mais je pense que cela vaut le coup d'en parler. Le DNS a été un vecteur dans ce cas pour cette attaque. Ce n'était pas le seul mais c'était un des vecteurs utilisés pour réaliser cette attaque.

Ensuite nous avons WannaCry dont on a déjà un peu parlé.

Avalanche. Avalanche état un service de nuage criminel. Donc imaginez, vous allez sur un site web, vous créez un compte, vous vous connectez, vous pouvez choisir le modèle, le type de campagne que vous voulez mettre en place. Et donc ils font tout pour vous. Vous ne deviez que leur payer et ils allaient tout mettre en place pour vous. Ils infectent pour vous vos consommateurs, ils vont créer un réseau zombie à votre place, ils vont vous fournir l'hébergement pour les cibles de distribution de logiciels malveillants,... Bref, ils font tout pour vous. C'est un niveau supérieur de sophistication en ce qui concerne les services criminels.

Avalanche a beaucoup utilisé le système de DGA, c'est-à-dire l'algorithme de génération de domaines. Alors quand les forces de l'ordre sont intervenues, il y a eu un processus au sein de l'ICANN. Le processus a donné lieu à la fermeture de plus de 1000 noms de domaine qui ont été retirés du web. Il y a eu donc un travail de concert entre l'ICANN et les forces de l'ordre. Et les criminels ont donc perdu contrôle sur cette infrastructure. Ils étaient là mais ils ne pouvaient plus contrôler ce type de domaines. Et c'était beau de voir cela.

Voilà certaines des chaînes qui ont été créées par Avalanche, par ce réseau zombie à des fins de commande et contrôle. Et vous voyez que parmi ces noms de domaine, il y avait pas mal de TLD.

Il y avait des ccTLD et des gTLD. Les criminels utilisaient ce qu'ils pouvaient à des fins malveillantes.

Un autre élément. Certains criminels dans certaines parties du monde vont créer leur logiciel malveillant de telle façon que ces logiciels ne puissent pas attaquer des adresses dans leur propre juridiction. Et donc ils n'attaquent pas les adresses IP qui sont dans leur propre juridiction parce que ces gens-là ne peuvent pas quitter leur pays. Donc ils se rendent prisonnier de leurs propres frontières. C'est bien qu'ils restent à leur place, mais ils font quand même beaucoup de mal.

Voilà les résultats d'Avalanche, la fermeture de site suite au démantèlement d'Avalanche. Europol, le FBI ont présenté un document sur cette affaire. Ici, nous voyons les principaux résultats : cinq arrestations dans quatre pays, 37 recherches dans sept pays, 59 serveurs saisis dans 13 pays, 221 serveurs hors lignes, 64 TLD/832 000 domaines dans 26 pays. C'était vraiment une opération à grande échelle et c'était vraiment quelque chose de très positif d'avoir pu démanteler un tel service.

WannaCry. WannaCry, si on voit cela depuis la perspective du DNS, contrairement à ce que l'on voit d'habitude lorsqu'on parle de types de logiciels malveillants qui utilisent les noms de domaine pour commander et contrôler, la commande et

contrôle de WannaCry était fournie par sept noms de domaine. .onion était défini par l'IETF pour qu'il ne soit jamais dans la racine, cela veut dire que l'ICANN n'avait rien à voir avec ce .onion. Donc il n'y avait pas moyen d'arrêter cette structure de commande et contrôle associée à WannaCry.

Or, il y a eu un chercheur, Marcus Hutchins, un chercheur très jeune, qui a pu obtenir un échantillon de WannaCry. Et c'était dans le code. C'était codé en dur dans le modèle. Et cette personne a pu décoder cela et arrêter la diffusion de ce logiciel malveillant. Et ce que vous voyez là-bas, c'est le raisonnement. Si mon rançongiciel ne peut pas se connecter au C2, alors ce serait sûr de chiffrer le système de la victime. Autrement, le rançongiciel ne peut pas se connecter à C2 et alors, le processus de sortie empêche toute analyse. Voilà un petit peu le raisonnement de WannaCry.

L'abus du DNS ou l'utilisation malveillante du DNS est un sujet assez controversé au sein de l'ICANN. Il y a différents points de vue pour ce qui est des côtés des forces de l'ordre. Il y a des inquiétudes en ce qui concerne l'exactitude du WHOIS et l'impact que le RGPD aura sur le WHOIS après le 25 mai, quand ce règlement entrera en vigueur. Il y a également des inquiétudes concernant le temps de réaction suite à l'identification d'un cas d'abus. Il y a différents types

d'inquiétudes pour ce qui est de la sécurité et de l'utilisation malveillante du DNS.

De l'autre côté, nous en tant qu'ICANN, en tant qu'organisation, on doit écouter ces inquiétudes. Mais l'ICANN ne peut pas sortir du cadre de son mandat, en ce sens que tout ce qui a trait au contenu ne rentre pas dans la portée du travail de l'ICANN. Les contrats de l'ICANN peuvent contenir des dispositions mais tout ce qui est lié au contenu ne peut pas être géré par l'organisation. Ce sont des discussions qui doivent avoir lieu chez vous. Nous pouvons faciliter ces discussions mais nous, nous ne pouvons pas y participer.

Le groupe de travail sur la sécurité publique regroupe les forces de l'ordre civils et militaires au centre de la structure de l'ICANN. Le PSWG, avant que ce groupe existe, les forces de l'ordre n'avaient pas vraiment une organisation ou un organe où se regrouper. Je pense que c'était à Beijing où la Commission fédérale du commerce a demandé à Fadi Chehadé si l'ICANN pouvait considérer la possibilité de créer une structure formelle pour regrouper les forces de l'ordre au sein de l'ICANN. Et Fadi leur a dit : « Présentez-moi une proposition. » Ils l'ont fait et cette proposition, c'est ce que nous connaissons aujourd'hui comme le PSWG, à savoir le groupe de travail. C'est un sous-groupe du comité consultatif gouvernemental qui s'occupe de la sécurité publique.

L'objectif de ce groupe est de fournir un avis au GAC, au comité consultatif gouvernemental, et un avis également à la communauté plus large de l'ICANN sur l'abus du DNS, les manières dont le DNS peut être utilisé à des fins malveillantes pour léser les utilisateurs car tout cela peut avoir des implications, que l'on le veuille ou non, sur l'information WHOIS.

La traduction des adresses de réseau CGN. De quoi s'agit-il ? Il s'agit d'une technique de certains fournisseurs de service internet quand ils préfèrent de ne pas migrer vers IPv6. Donc au lieu de basculer à IPv6, ils créent des réseaux locaux et ils attribuent des adresses IP dans ces zones. Les adresse IP doivent être dans l'internet public, tout ce que nous voyons quand on analyse le trafic. Et il y a des adresses IP qui peuvent exister seulement dans des réseaux privés et ces adresse IP ne devraient jamais être vues dans le réseau public. C'est ce qui se passe par exemple dans vos compagnies, dans vos maisons. Vos dispositifs ont des adresses IP privées.

Ce que fait le CGN, c'est que ces adresse IP sont allouées à leur consommateur et cela crée des espèces d'énormes réseaux locaux avec une seule adresse IP publique, ce qui crée une complication pour les forces de l'ordre parce que quand ils vont toquer chez quelqu'un pour voir qui est l'utilisateur qui a envoyé ce trafic de cette adresse IP à cette autre adresse IP, le

fournisseur de service internet ne peut pas dire de qui il s'agit parce qu'il y a X quantité d'utilisateurs qui utilisent une seule adresse publique. Et dans différents pays, il peut y avoir ou non des obligations en ce qui concerne le stockage d'archives de trafic. Alors dans certains pays, toutes les données de connexion ne sont pas stockées et le fournisseur de service internet ne sait pas si vous avez été là ou pas. C'est pourquoi le PSWG se penche sur cette question, sur cette technique car c'est une technique que les criminels peuvent utiliser.

Voici deux exemples simples qui ne sont pas restrictifs. Cette liste n'est pas exhaustive. On ne comprend pas toutes les dispositions contractuelles. Dans le grand réseau de contrats de l'ICANN, il y en a d'autres. On pourrait en discuter pendant des heures que pour aborder la lutte contre l'utilisation malveillante dans les sphères de l'ICANN. Je pourrais dire, bien sûr, que les opérateurs de registre sont tenus de surveiller leur zone pour voir s'il y a des menaces à la sécurité. Cela veut dire qu'ils sont obligés de vérifier les noms de domaine qui existent au sein de leur propre service.

Si moi j'étais le TLD .carlos, il faudrait que je m'occupe de voir si tous les noms de domaine hébergés sous le .carlos sont sécurisés ou s'il y avait des problème de rançongiciels, de logiciels malveillants ou quoi que ce soit. Donc c'est cela le devoir des opérateurs de registre. Si je ne me trompe, les

opérateurs de registre doivent également fournir les informations de personnes ou points de contact en cas d'abus, spécifiquement pour ce qui est de la lutte contre l'abus du côté des opérateurs de registre.

Pour ce qui est des bureaux d'enregistrement, ces exigences sont un peu plus spécifiques et ces dispositions plus spécifiques sont contenues dans un contrat que l'on connaît comme le contrat d'accréditation des bureaux d'enregistrement. À l'informel, on l'appelle RAA. Et ces dispositions plus spécifiques y apparaissent grâce à 12 recommandations des forces de l'ordre qui ont été formulées par ce que l'on connaît aujourd'hui comme le PSWG. À l'époque, c'était le GAC qui avait recommandé cela lors de la réunion du Costa Rica de 2012. Donc ils ont demandé au Conseil d'Administration de lancer des négociations à travers son personnel avec les bureaux d'enregistrement pour signer un nouveau contrat d'accréditation. Ces négociations on pris quelques mois et le résultat en est le RAA, qui a donc prévu ces dispositions plus spécifiques par rapport à la lutte contre l'abus.

Dans la communauté, on voudrait des fois avoir des dispositions un peu plus strictes mais à l'époque, les forces de l'ordre étaient d'accord avec ces dispositions pour l'organisation ICANN. Certaines de ces obligations, je les aborderai rapidement, comprennent par exemple que les bureaux d'enregistrement

doivent prendre des mesures raisonnables au moment de recevoir des informations d'un abus. Lorsqu'on leur demande ce qui est raisonnable, bien sûr les avocats vont toujours avoir des réponses différentes, ce qui rend les choses un peu plus compliquées. Mais en tout cas, c'est ce qui est contenu dans le RAA.

Une autre obligation des bureaux d'enregistrement est de fournir leurs informations du point de contact en cas d'abus, informations qui doivent être soit publiées sur le site web, soit contenues dans les données du WHOIS. Je pense que dans les données du WHOIS, il faut également publier ces informations sur leur site web. Comme vous voyez, je n'en suis pas tout à fait sûr. Je pense que c'est le cas mais je n'en suis pas sûr.

Il y a également une disposition intéressante qui porte spécifiquement sur l'application de la loi. Donc lorsque les forces de l'ordre envoient à un bureau d'enregistrement dans leur propre juridiction une signalisation d'abus, toujours dans la même juridiction rappelez-vous, le bureau d'enregistrement doit fournir une réponse humaine dans les 24 heures, c'est-à-dire que cette réponse doit être envoyée par une personne. On ne peut pas envoyer de réponse automatique. La réponse ne peut pas être « On a mis ce nom de domaine en suspension. » Cela peut être « Merci, on en prend note. » et on envoie un accusé de réception et ça y est. Mais la personne qui réponde

devrait être quelqu'un qui puisse décider de ce que cette signalisation d'abus génèrera, que ce soit une mise en suspension ou pas.

Ces dispositions sont très utiles dans certains cas lorsqu'il y a beaucoup de bureaux d'enregistrement, par exemple, qui exploitent des services dans la même juridiction mais dans certaines juridictions, il n'y en a pas beaucoup ou il n'y en a pas tout court. Donc cette disposition, bien sûr, va varier et l'effet de cette disposition varie selon la juridiction.

On a également des fournisseurs de service d'enregistrement fiduciaire et des services de confidentialité, donc d'anonymisation. Et il se pourrait qu'il y ait quelqu'un qui donne ses propres informations dans les données WHOIS plutôt que les données de la personne qui est le vrai titulaire du nom de domaine. Donc ces fournisseurs de service d'anonymisation d'enregistrement fiduciaire doivent également fournir leurs propres informations de point de contact au bureau d'enregistrement.

Je pense en être à la fin de ma présentation. J'ai abordé tous les sujets que je voulais aborder. C'est un domaine d'informations très vaste, l'abus des noms de domaine. Lorsque vous voyez un nom de domaine qui est utilisé pour les fonctions de commande et contrôle d'un réseau zombie, il est tout à fait clair que ce nom

de domaine fait l'objet d'un abus. Lorsque vous voyez des analyses techniques et que l'on ne peut pas aller à l'encontre de ces évidences techniques, on a des déterminations plus claires. Mais dans certains cas, il y a un peu plus de doutes. Donc ce sujet, bien sûr, peu être discuté davantage. Cela appartient à la communauté de continuer, de se pencher sur ces sujets et de continuer d'y travailler.

Comme je l'ai dit au début, je suis le directeur de la sécurité, de la stabilité et la participation au sein de l'équipe de sécurité et stabilité au sein de l'équipe de CTO. Nous participons beaucoup avec la communauté de la sécurité des forces de l'ordre et nous essayons de faire énormément de travail. On essaie de se rapprocher du monde de l'ICANN. Nous sommes très intéressés par cette possibilité qui comprend les discussions qui se tiennent ici. Il y a quelques semaines, un représentant de l'industrie des noms de domaine a assisté à une conférence sécurité suivant notre propre invitation. Le représentant était Jonathan Frakes, le directeur exécutif de l'association des noms de domaine. Il a eu des interactions très enrichissantes. Et cela fait partie de notre travail. Nous communiquons avec ces personnes, nous essayons de les impliquer, ces personnes qui ne se connaissent peut-être pas. Donc on essaie de les réunir pour qu'ils se comprennent entre eux de manière à ce que tout le

monde sache ce que font les autres et que sur ces fondements, l'on puisse ensemble développer des solutions.

On travail également avec les forces de l'ordre. Comme vous vous souviendrez, l'un des devoirs de l'ICANN, l'une de ses missions est d'aider à maintenir la sécurité, la stabilité et la résilience du système des noms de domaine, c'est-à-dire que l'application de la loi et les forces de l'ordre en particulier doivent comprendre s'il s'agit d'une enquête par rapport à la distribution d'un logiciel malveillant ou s'il s'agit d'un cas de criminalité. Donc on essaie de les aider à comprendre si la sécurité, la stabilité et la résilience, ou SSR comme on l'appelle au quotidien, est attaqué, s'il a des compromis à ce niveau-là.

Donc voilà. Si vous avez des questions, allez-y.

CATHY PETERSEN : Je vous rappelle de dire vos noms et votre organisation, s'il y en avait.

ORATEUR NON-IDENTIFIÉ : Bonjour, je suis [Marsy] de l'Inde. Moi, j'ai un commentaire et une question. Je voudrais savoir si l'ICANN a élaboré des lignes directrices de base pour la mise en place de ces mesures au niveau de l'opération – cela pourrait être des dispositifs qui n'ont pas de couche de sécurité ou il pourrait y avoir différentes

menaces – et si vous avez des mesures d'analyses postérieures. Donc si avant de lancer un DNS, de le mettre en opération, il y a des lignes directrices à suivre.

CARLOS ALVAREZ : Je suggère que consulter DNS-OARC. C'est la communauté des opérateurs de DNS. Il y a des normes, bien sûr, qui pourraient être liées à ces données de déploiement. Et puis cherchez le M3AAWG. Il y a un an et demi à peu près, ils ont mis à jour ce que l'on connaît comme... Attendez. Si vous cherchez M3AAWG DNS threats en anglais ou menace, vous êtes sûr de le trouver. Mais en tout cas, je pense que ces communautés ou ces groupes ont des documents qu'ils ont élaborés par rapport à ce que vous demandez.

ORATEUR NON-IDENTIFIÉ : Je voudrais voir des lignes directrices, c'est cela que je voudrais savoir, s'il y a des lignes directrices pour ces normes de sécurité minimum et pour les mettre en œuvre.

CARLOS ALVAREZ : Cela ne peut pas être exigé. Toutes les personnes autour du monde peuvent le faire. Il n'est pas possible, en fait, de le mettre en application. C'est quelque chose qui est impossible d'éviter. Il

n'y a pas de règle, il n'y a pas d'obligation ; c'est quelque chose de volontaire. Et ce n'est pas simple, vous imaginez.

Par rapport à ce que vous disiez, il y a une composante volontaire. Donc il y a des normes et des moyens de faire les choses qui ont été définies par la communauté technique depuis très longtemps, depuis 1997 par exemple, avec l'exfiltration des ports d'adresse IP. Si vous cherchez le BCP 38 ou le BCP 34, vous verrez que ces meilleures pratiques en vigueur datent de beaucoup d'années. Mais c'était de bonnes pratiques qui durent toujours et qui, pourtant, n'ont pas été mises en œuvre partout parce que c'est quelque chose de volontaire, justement.

Y a-t-il d'autres questions ? Oui, monsieur, allez-y. Votre nom s'il vous plaît ?

HARU AL-HASSAN : Je m'appelle Haru Al-Hassan, je viens du Nigéria. Dans les pays en développement, nous avons un défi au niveau de la formation des forces de l'ordre pour qu'elles puissent être à la hauteur de la lutte contre les délinquants parce que vous avez démontré qu'il y a énormément de manières d'empoisonner le DNS ou de l'attaquer. Donc comment pourrions-nous former nos forces de l'ordre pour qu'elles soient à la hauteur de ce défi, de lutter contre les délinquants ?

CARLOS ALVAREZ : Je pense que vous devriez contacter le personnel de participation de l'ICANN en Afrique. Vous avez un vice-président de l'Afrique ici, je ne sais pas si vous l'avez déjà rencontré, mais peut-être que vous pourriez manifester cela auprès de cette personne, lui exprimer cette inquiétude. Par la suite, Pierre avec notre équipe pourrait coordonner un atelier pour que les forces de l'ordre participent à une séance de formation sur l'abus du DNS. Donc je vous conseillerais de contacter Pierre parce que votre inquiétude est tout à fait valable.

Oui, monsieur ?

BRENT CAREY : Je suis Brent Carey de .nz. Je me demande si vous avez des liens avec la juridiction et l'internet. Je suis entré d'Ottawa la semaine dernière et il y avait des informations d'abus de contenu, d'enregistrement DNS et ce sont des sujets qui commencent à apparaître. Donc je me demandais si vous avez des liens que vous pourriez partager avec nous ?

CARLOS ALVAREZ : Non. C'est étrange. Je n'en ai pas. Mais oui, je sais que Bertrand a organisé ce forum à Ottawa. Certains de mes collègues de l'ICANN y ont participé.

BRENT CAREY : Parce qu'il y avait beaucoup d'inquiétudes par rapport à cela.

CARLOS ALVAREZ : Très bien. Je n'en étais pas au courant. Peut-être que cette conversation devrait être tenue avec le PSWG. Merci.

Bien. On a une autre question.

ORATEUR NON-IDENTIFIÉ : Je voudrais savoir ce que vous attendez comme mécanismes qui soient mis en place à la lumière du RGPD pour le WHOIS et quel est, à votre avis, le chemin à suivre ou quelle sera la situation dans l'avenir.

On n'a pas un WHOIS authentique. Peut-être qu'à la lumière de ce RGPD, on pourra voir qui est la personne, où on avance, dans quel sens on avance. On n'a pas de contrôle par rapport au WHOIS en ce moment. Donc peut-être que grâce à ce RGPD, cela pourrait changer. Qu'en pensez-vous ?

CARLOS ALVAREZ : Il faudrait attendre. Je vous conseille de participer à ces discussions, de faire vos contributions lors des appels de l'organisation ICANN. En général, c'est le PDG qui lance ces appels à contribution à la communauté. Donc participez. C'est

comme cela que vous pourrez vous faire entendre. Et on vous écoute ; on écoute. Je ne dis pas cela comme cela. Manifestez cette inquiétude.

À l'écran, je partage avec vous quelques séances. Ce ne sont pas les seules séances d'intérêt pour ce qui est de l'abus du DNS, sachez-le. Peut-être que vous pourriez chercher les procès verbaux d'hier. Hélas, on ne peut plus assister à cette séance, elle est déjà passée. Mais demain, vous aurez la réunion du PSWG du GAC, et le GAC et le PSWG qui aborderont le RGPD et le WHOIS demain matin. J'ai une préférence par rapport à la séance qui concerne le RGPD parce que nous sommes en ce moment devait justement cette question, c'est ce qui est en vogue en ce moment.

Il y a également [l'ADN] et l'initiative des domaines qui ont une bonne santé. C'est une séance intéressante. Ils sont en train de beaucoup travailler. Et puis on a le DAAR jeudi qui est un outil qui a été développé par mon équipe, un outil qui fournit des informations sur les enregistrements et sur comment ces mauvais enregistrements rajoutent aux surcharges à un secteur plutôt que de distribuer la charge parmi certains noms de domaine. Donc je vous conseille d'y assister et de vous amuser.

Merci d'être venus.

CATHY PETERSON : Donc pour rappel, les présentations sont déjà publiées sur le programme public pour cette séance. Nous y ajouterons les procès verbaux et les enregistrements de cette séance dans l'emploi de temps public dans les prochains jours. Donc vous pourrez revenir là-dessus pour consulter toutes ces informations. Merci.

Nous allons avoir notre prochaine séance sur « Comment cela fonctionne », l'explication sur les réseaux d'internet à 15:30. On prendra un tout petit peu de retard, on ne commencera pas à 15:15. La séance sur l'internet abordera l'IPv4, l'IPv6 en tant que protocole. Donc j'espère que vous aurez le temps de rester. Allez chercher un café et revenez. Merci.

[FIN DE LA TRANSCRIPTION]