JOHANNESBURG – Session 2 de renforcement des capacités des ALS de l'AFRALO d'At-Large
Mardi 27 juin 2017 – 08h00 à 09h00 JNB
ICANN59 | Johannesburg, Afrique du Sud

AZIZ HILALI : Bonjour à tous. Bienvenue à cette deuxième session sur le renforcement de capacités que nous organisons chaque jour à 8 heures du matin. Le thème d'aujourd'hui sont les défis en matière de sécurité ayant un impact sur les titulaires de nom de domaine et les utilisateurs finaux. Un sujet très important, et c'est pour ça qu'on a voulu que cette deuxième soit réservée à ce thème.

J'ai le plaisir de vous présenter les deux intervenants que je remercie en votre nom d'être présents avec nous pour cette session de renforcement de capacités. Il s'agit de Steve Sheng, à ma gauche, directeur du soutien à l'élaboration des rapports consultatifs du SSAC – il expliquera ce que c'est – et du RSSAC, et monsieur David Piscitello – j'espère que je le prononce bien – qui est vice-président au niveau de la sécurité et le coordinateur de tout ce qui est ICT. Je les remercie et je vais passer tout de suite la parole à Steve Sheng, tout en le remerciant. Merci.

STEVE SHENG : Merci beaucoup, monsieur le Président de séance. Je m'appelle Steve et je suis très heureux d'être ici avec vous, ce matin. C'est la troisième fois que je viens en Afrique, et à chaque fois je me sens accueilli chaleureusement et je me sens chez mo, même sur le vol de la compagnie South African.

Je travaille donc dans le département des politiques et notre équipe soutien le développement et le conseil pour la sécurité et la stabilité de l'Internet, ainsi que pour le système de serveur.

À ma gauche, nous avons David qui va se présenter lui-même. C'est un ancien collègue. David ?

DAVID PISCITELLO : Bonjour. Je m'appelle David Piscitello et je suis vice-président de la sécurité et coordinateur ICT de l'ICANN. Je travaille avec le responsable informatique pour la sécurité et la stabilité de l'Internet.

STEVE SHENG : Nous voulons travailler de manière interactive et nous voulons nous concentrer sur les titulaires de noms de domaine et les utilisateurs finaux un peu. Mais j'aimerais commencer par mettre tout cela en contexte.

Lorsque l'on réfléchit aux menaces sur la sécurité, ça peut être divisé en trois catégories. La première catégorie, ce sont les attaques physiques. Ce sont des attaques sur l'infrastructure même. L'infrastructure des télécommunications, couper les câbles, des attaques physiques donc, matérielles.

Deuxième type d'attaques, les attaques syntactiques. Ce sont des attaques du protocole de fonctionnement, attaquer les points faibles, les vulnérabilités. Vous avez par exemple des attaques comme le ransomware où on utilise les failles de Windows pour insérer des demandes de rançon, on l'a vu aux informations, demander des fonds, lorsqu'on bloque les ordinateurs et on demande de l'argent pour les débloquer. Une attaque néfaste, nuisible, ça va être aussi de lancer un flot de données pour là aussi bloquer la communication. Donc les attaquants essaient de contrôler la situation. Ces attaques syntactiques consistent à s'attaquer au protocole, à la conception même des systèmes.

Donc on a les attaques physiques, les attaques syntactiques et la troisième catégorie, les attaques sémantiques. Ce type d'attaques sémantiques a à voir avec la manière dont les êtres humains attribuent la signification. Je vais vous donner un exemple, le hameçonnage. Dans ce contexte, un attaquant s'en prend à un site Web et vous présente ensuite un site Web comme s'il venait d'une source légitime. Donc l'utilisateur final

croit qu'il est sur un site Web normal avec un contenu légitime et il fait confiance à ce site Web et lui donne des informations.

Donc ces trois types d'attaques nous connaissons, ces trois variantes se font sur différents continents mais différemment. En Asie par exemple, les attaques d'ingénierie sociale ne se font pas avec de nouveaux sites Web mais utilisent notamment les téléphones portables ou simplement communiquent avec vous. Ça dépend du continent. Je ne connais pas bien, comme je vous l'ai dit, ce qui est plus prévalant en Afrique, mais je veux vous montrer quel est le contexte de ces problèmes pour que vous puissiez mieux comprendre la situation des tendances de sécurité. Nous allons donc passer en revue cette présentation.

Lorsque l'on parle de menaces, de menaces pour les titulaires de noms de domaine, les personnes qui ont inscrit un nom de domaine, qui ont peut-être même un portefeuille de plusieurs noms de domaine, il y a deux types de menaces. Des menaces externes et des menaces internes.

Au niveau des menaces externes, imaginons un attaquant qui va être actif, cette organisation va tenter d'accéder à votre compte pour le contrôler, contrôler votre nom de domaine, votre inscription à un nom de domaine. Vous avez fait une inscription auprès d'un bureau d'enregistrement, vous passez par des

revendeurs, et il y a des attaques sur ces comptes pour contrôler les noms de domaine.

Quelque chose de similaire également est d'essayer d'obtenir l'accès à votre compte une fois de plus pour altérer les informations du DNS associées à votre nom de domaine. Qu'est-ce que je veux dire par là ? Vous enregistrez un nom de domaine, vous êtes présent sur le Web, vous avez peut-être votre adresse email basée sur votre site Web, et lorsqu'un attaquant accède à cela, il ou elle va insérer des nouvelles données, changer l'adresse de protocole Internet, l'IP, là où doit aller votre correspondance courriel, par exemple, et il va vouloir éventuellement utiliser votre compte comme base pour conduire une attaque pus large. Ou bien il va s'attaquer à votre site Web ou il va demander de l'argent. Ça, ce sont les attaques externes.

Au niveau des attaques internes, et là les noms de domaine ont une valeur résiduelle et une réputation. Lorsque vous vous inscrivez auprès d'un nom de domaine, cela a une valeur. Dans certains cas, ça coûte cher de changer de nom de domaine, de passer à un autre nom de domaine. Parce que vos noms de domaine ont une valeur, il y a des gens qui vont surveiller de près votre nom de domaine et parfois vous oubliez de renouveler votre inscription. Il y a cette période de cinq jours qui s'écoule, vous savez, et il y a quelqu'un qui va essayer pendant

ces cinq jours de s'enregistrer en utilisant votre nom, et à ce moment-là, il vole votre nom de domaine et il lui appartient. Ensuite, c'est un processus très long d'essayer de récupérer votre nom de domaine.

Je vais rentrer plus en détail maintenant dans ces menaces. Donc on a parlé d'accès non autorisé sur le compte d'inscription au nom de domaine, d'enregistrement du nom de domaine. Comment les gens malveillants procèdent-ils ? Ils devinent, ils essaient de deviner votre nom et votre mot de passe.

Vous vous dîtes, ce doit être impossible de devenir mon mot de passe, mais moi j'ai fait une étude lors de mon doctorat sur les systèmes de sécurité et en fait, pour les mots de passe, c'est plus simple que cela en a l'air. Les gens utilisent plusieurs fois les mêmes mots de passe ; pour votre banque, pour votre courriel, vous réutilisez tout le temps le même mot de passe. Ce qui veut dire que quelqu'un qui vous attaque va essayer, peut-être qu'il connaît déjà un de vos mots de passe, donc il va le réutiliser.

Deuxième faiblesse, il y a entropie pour les mots de passe. Est-ce difficile de deviner un mot de passe ? En fait, c'est très facile. Mon professeur à l'université avait fait un poster d'une dizaine de milliers de mots de passe, et on les a analysé. Il y avait les « I love you », les plus courants, ceux que l'on trouve facilement.

Donc, ces attaquants sont en mesure très facilement de deviner vos mots de passe.

David.

DAVID PISCITELLO : Est-ce que vous avez plus de sept caractères dans votre mot de passe ? Levez la main. 10 caractères ? Vous gardez la main levée, pas mal. 15 caractères ? Vous savez, à l'ICANN on a 20 caractères, c'est difficile, c'est très long. 20 caractères au moins à l'ICANN, pour sécuriser.

Avez-vous un gestionnaire de mots de passe sur votre ordinateur ? Un logiciel qui gère vos mots de passe ? Vous êtes un pro, vous. Utiliser un système de gestion de mots de passe génère de très solides mots de passe pour vous et ça les conserve de manière sécurisée sous forme cryptée dans votre ordinateur. Il y a pour Androïd et pour iPhone, il y a également ce genre de systèmes. C'est très utile.

Je voulais également signaler que deviner les mots de passe, ce n'est pas le plus facile pour les attaquants, mais ce qu'il y a d'encore plus facile, c'est compromettre une base de données avec les sites Web que vous avez visités. S

Comme l'a dit Steve, si vous avez créé un mot de passe, vous l'avez utilisé très souvent ailleurs, donc ils vont sur des milliers

de sites et utilisent votre adresse email pour essayer d'appareiller les deux – votre adresse email et vos mots de passe – et ils obtiennent ainsi des informations. C'est pour cela qu'il est essentiel de ne pas utiliser le même mot de passe pour votre banque, ça doit être séparé. Si vous avez plusieurs banques, utilisez plusieurs mots de passe également.

STEVE SHENG : Merci beaucoup, David. Je poursuis un peu.

Il peut donc y avoir capture à partir d'un hôte, ça peut être sur votre ordinateur ou directement sur le serveur que l'on vole les mots de passe. Par exemple, ma femme avait mis sur un fichier Word tous les mots de passe – je vous assure. Et comme David l'a mentionné, il y a également les systèmes de gestion de mots de passe.

On a parlé de hameçonnage et c'est la première étape, le hameçonnage de plus en plus ciblé. Ils essaient d'installer un logiciel malveillant qui va capturer toutes vos frappes et intercepter ce que vous envoyez avec votre ordinateur. Donc, à un moment, vous recevez un courriel de votre bureau d'enregistrement vous disant qu'il y a des activités non autorisées sur votre compte. Ça vous est peut-être déjà arrivé. Alors vous vous dîtes « Bon, ok » – on vous dit « veuillez vous connecter pour confirmer toutes vos données ». C'est assez

commun. Bien entendu, ça ne vient pas du bureau d'enregistrement.

Vous pouvez compromettre votre ordinateur également en téléchargeant des documents, ce qui installera alors des logiciels espions sur votre ordinateur et vous en connaissez les risques.

L'accès non autorisé, c'est donc la première étape. C'est un moyen, mais ce n'est pas une fin. Quel est le but recherché ? Essayer de modifier vos informations de configuration du DNS, donc changer le nom de votre serveur, l'adresse IP, et alors votre service va s'interrompre. Le trafic sera redirigé vers le serveur de l'attaquant.

Il peut aussi y avoir des erreurs administratives qui auront des conséquences assez similaires.

Un autre aspect qui apparaît comme un précurseur de l'attaque, c'est quand on essaie de changer les informations pour tenter une nouvelle fois de prendre le contrôle de votre nom de domaine. C'est du piratage. C'est pour cela qu'on appelle cela du piratage de noms de domaine, c'est de l'usurpation de nom de domaine.

Ce que fait l'attaquant, c'est changer tout de suite votre adresse email par laquelle les bureaux d'enregistrement vous

contactent. Vous vous basez donc sur cette communication avec le bureau d'enregistrement pour recevoir des informations importantes, or là vous ne recevez plus d'informations. Beaucoup d'entre nous oublient, parce qu'on reçoit déjà bien trop de courriels chaque jour, dans la plupart des cas.

Mais lorsque ce sont les mauvaises informations pour le DNS, il va y avoir des inexactitudes sur le WHOIS, ce qui peut mener à la suspension du nom de domaine ou à son annulation. Avec ces nouveaux contrats qui existent, le WHOIS doit être exact, sinon votre nom de domaine ne sera pas maintenu et vous pouvez être suspendu. Vous serez considéré comme une personne non autorisée.

Voilà en gros le type de risques qui existent au niveau de la sécurité pour les titulaires de noms de domaine DNS.

J'aimerais maintenant ouvrir aux questions. Avez-vous des questions sur ma présentation ?

GABRIEL BOMBAMBO BOSEKO : Je voudrais savoir si l'ICANN prend des précautions – c'est Gabriel Bombambo, je viens du Congo-Kinshasa – je voulais savoir si ICANN prend des précautions pour, en quelques sortes, punir les gouvernements qui font des attaques externes auprès des utilisateurs finaux, un utilisateur

final comme chez nous où il y a beaucoup d'opposants politiques, son site ou ses données pourraient être attaqués, si c'est avéré que cela vient du gouvernement. Quelles mesures prendraient l'ICANN envers pareil gouvernement ?

STEVE SHENG : Je vais être bien sûr d'avoir compris votre question. Vous nous décrivez une situation où un gouvernement attaque un utilisateur final dans son propre pays ou dans un autre pays ? Ce sont deux choses différentes, c'est du terrorisme d'un côté ou de l'oppression de l'autre, quand c'est le même pays.

Nous n'avons pas de rôle à jouer à ce niveau. Notre rôle, même dans le domaine de la sécurité, est de faciliter et de conduire un travail d'expert, de spécialiste.

Si nous travaillons avec un gouvernement, ça va être en rapport avec le ccTLD, le nom de pays, par exemple on a un rapport avec des noms de domaines ccTLD, noms de domaine de pays qui font partie du DNS. Donc on peut recevoir des courriels, il y a des utilisateurs finaux qui utilisent ce nom de domaine et ça doit bien fonctionner. On travaille à ce niveau. C'est notre rôle principal dans la fonction IANA qui s'appelle maintenant PTI, l'IANA suite à la transition.

Mon équipe, au niveau opérationnelle, nous travaillons principalement à des menaces contre le DNS au niveau mondial, au niveau global. On travaille avec des gouvernements si un site Web est attaqué. Par exemple, en Géorgie, tous leurs sites Web ont été attaqués et nous les avons aidés au niveau de la sécurité opérationnelle mais nous, on ne rentre pas dans des conflits ou des confrontations entre gouvernements et utilisateurs.

AZIZ HILALI: Deux questions, ou plutôt une remarque pour la première, à propos du typosquattage, nous avons le même mot en français, c'est quand des malveillants utilisent le fait qu'une personne tape un nom de domaine, ils jouent sur les fautes qui peuvent avoir lieu sur un nom de domaine. Par exemple s'il y a un ou deux « t » pour donner à l'utilisateur l'impression qu'il se trouve sur un site alors que ce n'est pas le cas. Ça pose particulièrement souci dans les cas de hameçonnage, on a l'impression qu'on est sur la page d'une banque avec le logo, etc.

Deuxième question, en rapport avec la question de Gabriel. Lui il a posé la question entre gouvernement et citoyen, moi je voudrais aussi savoir quels sont les dangers qu'on court au niveau des élections, particulièrement en cas d'attaques entre

deux états, comme c'est supposé être ce qui s'est passé aux États-Unis.

DAVID PISCITELLO : Permettez-moi de répondre à la première question. Je crois que vous parlez de cybersquattage, et il y a des lignes de conduite et des règles pour ce typosquattage. Le nom peut donc être retiré du DNS, le mauvais nom, et il y a en effet des menaces qui existent et qui évoluent à partir de ce typosquattage. On réécrit la résolution des noms de domaine et ça, c'est parfois fait par des entités commerciales.

Par exemple, un hôtel ou un café qui offre l'Internet gratuit et disponible qui veut gagner de l'argent sur vos fautes de frappe. Si vous faites www.ebay,com, un service ou un kiosque dans un hôtel qui va prendre la réponse de l'Internet disant « il n'y a pas de noms de ce type », ce qui vous redirigera vers une page, un moteur de recherche qui va promouvoir d'autres services et fera de la publicité, ce n'est pas exactement là que vous vouliez aller mais vous avez l'impression d'avoir fait une faute de frappe, ce qui vous renvoie ailleurs. Il y a eu un rapport là-dessus il y a de cela quelques années et j'ai écrit un article à ce sujet. C'est vraiment mauvais parce que c'est un mensonge. Ça vous renvoie à un endroit où vous n'étiez pas censés aller.

Il faut donc être bien conscient de cela, et si vous travaillez dans un café avec Internet gratuit, faites attention. Il faut bien configurer votre ordinateur portable pour toujours utiliser un serveur de confiance, par exemple Google, un moteur de recherche réputé, Google c'est 8.8.8.8. Vous pouvez configurer votre portable là-dessus de manière statique et où que vous alliez, vous serez sûr d'aller sur Google, et on ne vous mentira pas et on ne vous enverra pas vers un site publicitaire.

STEVE SHENG : Je vais essayer de répondre à la deuxième question concernant ces élections, le hameçonnage, les attaques de sécurité dont on a tant parlé pour les utilisateurs finaux. Le vol de courriels, ça c'est arrivé au plus haut niveau et cela dépasse le cadre des attributions de l'ICANN qui est là pour coordonner les identifiants.

Néanmoins, même notre organisation doit suivre ces formations et en tant qu'employé, nous devons être prudent pour ne pas être la victime de hameçonnage ciblé. Je peux vous donner quelques conseils un peu plus tard, mais cela n'est pas vraiment le travail de l'ICANN, d'éduquer les utilisateurs finaux sur ce type d'attaques.

DAVID PISCITELLO : Nous n'avons pas ça dans nos attributions, mais ce que fait mon équipe est de publier périodiquement des articles sur la terminologie de la sécurité. Par exemple, aujourd'hui, sur le Dark Web, je suis en train de faire un article, nous publierons des articles sur ce type d'attaques, vous pourrez les lire sur le blog de l'ICANN sécurité. C'est nous qui écrivons beaucoup de ces articles informatifs, vous trouverez beaucoup d'informations sur le site Web de l'ICANN. C'est parfois assez technique mais on essaie de vous faire comprendre les différentes menaces.

AZIZ HILALI : [Nous avons encore des gens qui veulent] poser des questions, je demande donc au personnel de faire des questions et des réponses rapides.

Tijani d'abord, puis Saïd, ensuite Bakary. Tijani.

TIJANI BEN JEMAA : Je pense que maintenant Steve l'a dit, mais quand vous avez répondu à la question de Gabriel, vous n'avez pas dit que ce n'était pas dans les responsabilités de l'ICANN. L'ICANN est responsable de la sécurité des identifiants uniques, de la racine et du serveur, et sous sa responsabilité, tout ce qui dépend de l'utilisateur du gouvernement et des bureaux d'enregistrement,

le contrat est entre l'utilisateur et le bureau d'enregistrement et ICANN n'intervient pas et n'a rien à faire au milieu. Merci.

DAVID PISCITELLO : Je voudrais vous corriger concernant la sécurité du serveur racine. ICANN n'a pas la responsabilité de cela. Nous avons la responsabilité de l'intégrité de la zone racine. Chacun des opérateurs de serveur racine est responsable de sa propre opération. Donc l'ICANN est responsable d'une partie et nous prenons cela au sérieux, nous faisons du très bon travail, mais le département de la défense des États-Unis et les autres sont responsables des opérations de leurs propres services de racine.

AZIZ HILALI : Saïd.

SAÏD MCHANGAMA : Merci. Saïd Mchangama, président de la fédération des consommateurs ALS aux Comores.

Moi, en tant que représentation des consommateurs, ce que je veux demander c'est est-ce que l'ICANN a des statistiques qui affinent le type de danger par région ? C'est-à-dire que je me dis que si aujourd'hui je devais faire une campagne de sensibilisation sur la sécurité, on peut souvent se dire qu'en

Afrique, il n'y a pas tant de danger, etc., donc est-ce qu'il y a des statistiques qui affinent un peu par région et par activité à la fois, qui nous permettent de dire « attention, ce n'est pas parce que vous êtes aussi riches que Google et les autres qu'il ne faut pas faire attention parce que vous utilisez ci ou ça ». Merci.

STEVE SHENG : Si j'ai bien compris votre question, de la perspective d'ICANN, avons-nous des données sur les menaces pour chaque région ? Des statistiques ? Je ne pense pas, parce que dans certains cas, comment obtenir ces données ? Nous ne savons pas. Nous avons une responsabilité limitée et certaines de ces données sont des données qui dépendent de compagnies de sécurité qui les possèdent, et certains bureaux d'enregistrement peuvent les avoir. Mais ce n'est pas très facile à obtenir. Donc je vais y réfléchir, mais je reconnais que c'est une bonne question, en tout cas. Laissez-moi y réfléchir et j'essaierai de vous donner un peu plus de précisions.

DAVID PISCITELLO : Je dirais que l'ICANN n'a pas ce type de données au niveau régional, mais si vous allez voir le groupe de travail anti-hameçonnage, je sais qu'ils ont peut-être ce type de données.

Il y a un rapport un peu ancien mais à une époque, je sais qu'une des menaces importantes pour la région africaine, par exemple, était les systèmes d'exploitation des téléphones mobiles en Afrique, parce qu'on ne fournissait pas de mise à jour automatique pour certains logiciels des utilisateurs finaux. Beaucoup de ces appareils sont très vendus en Afrique, parce qu'on essaie de maintenir des prix bas, les systèmes ne sont pas mis à jour et ça devient dangereux parce qu'ils deviennent vulnérables. Toute la population de cet exploitant est vulnérable. Chaque pays peut essayer de réduire le danger de ses utilisateurs en créant des normes obligatoires pour les télécoms, pour les responsables de ces téléphones portables pour que ces systèmes soient mis à jour.

C'est un défi parce que c'est une question économique ici. Si vous voulez qu'un téléphone soit disponible à un prix réduit pour la population, on mettra une mémoire plus réduite sur cet appareil et à ce moment-là, on ajoutera des fonctionnalités avec une petite mémoire, on essaiera de répondre aux besoins d'une population avec un appareil bon marché. On aura alors des problèmes de sécurité sur ces appareils. Donc une série de pays ont des problèmes technologiques en ce sens.

J'essaie de réfléchir un peu à cela. Je sais qu'il y a des statistiques régionales. Samantha en a. Il y a des statistiques sur les menaces au niveau régional. En général, beaucoup de

compagnies essaient de promouvoir la sécurité afin d'éviter les systèmes de logiciel de rançon.

Savez-vous ce que sont ces logiciels de rançon ? Ces attaques de logiciels de rançon consistent en une attaque email. Vous recevez un document par email, lorsque vous cliquez, un logiciel est installé sur votre ordinateur. Ensuite, un logiciel de chiffrement est téléchargé et va chiffrer toutes les données sur votre ordinateur, on va verrouiller votre écran, votre ordinateur, souvent en imitant une autre attaque. Vous devez alors payer une rançon à cette organisation qui vous réclame de l'argent pour pouvoir récupérer vos données. Cet attaquant va vous dire « Si vous ne payez pas cette rançon, vous ne pourrez pas obtenir vos données. Si vous payez la rançon, vous aurez une clef pour récupérer vos données ».

Si cela vous intéresse, nous n'avons pas beaucoup de temps aujourd'hui mais j'ai écrit des articles là-dessus. J'ai fait une présentation à ce sujet que je peux donner aux membres d'ALAC qui vous la donneront.

Il y a une attaque importante mondiale. Ils ont fait un bon travail pour la localiser en fonction des langues et des scripts locaux. Les écrans sont en arabe, en français, ce sont des attaques locales très sophistiquées dans la langue locale qui ont été réalisées.

AZIZ HILALI : Deux personnes dans la queue, ainsi que des remarques et des questions sur le chat, donc on va essayer de faire vite s'il vous plaît.

SERGE-PARFAIT GOMA : Bonjour tout le monde, je suis Serge-Parfait Goma, de Conga-Brazzaville. J'ai deux questions que je vais poser en une seule fois.

Ma première question, c'est est-ce que l'impact de la mise en œuvre de l'IPv6 consiste réellement une faille sur le DNS, que ce soit le DNSSEC, si oui quelle approche pour pouvoir palier à ça ?

Ma deuxième question concerne l'idée de la mise en place d'un observatoire sur les problèmes de sécurité dans les pays. Est-ce que l'ICANN peut accompagner de telles initiatives ?

Merci.

STEVE SHENG : Pour votre deuxième question sur la possibilité de créer un système de surveillance, un centre de surveillance, je dirais que ce n'est pas de la responsabilité de l'ICANN, loin de là. Les ressources qui pourraient être disponibles en ce sens appartiennent à l'équipe de réponse en cas de menace

informatique. Ils ont des centres dans beaucoup de pays. Aux États-Unis, vous avez un centre de coordination qui travaille dans ce domaine. Donc si vous voulez chercher quelque chose dans ce sens, je vous encourage à les contacter, à leur demander leur aide car ils pourront vous aider.

DAVID PISCITELLO : L'ICANN ne gouverne pas l'ICANN, ICANN est seulement un administrateur et il délègue la responsabilité de l'identificateur, donc une des choses que nous allons faire, c'est donner la responsabilité du nom de domaine aux registres de premier niveau qui sont responsables.

Verisign est par exemple responsable de .COM. Ils ont un contrat. On ne peut pas leur dire « Vous devez annuler ou supprimer ce nom de domaine », ce sont les forces de l'ordre qui doivent le faire directement avec Verisign.

Ça c'est pour vous donner un peu le contexte de ma prochaine réponse. Le type de menaces que nous contrôlons au sein de l'ICANN à travers notre centre opérationnel consiste en des défaillances du système des noms de domaine au niveau de la racine.

Donc, au niveau de l'ICANN, nous avons un système qui nous permet de contrôler et de vérifier ce qu'on appelle le serveur de

nom d'autorité pour tous les TLDs en fonctionnement, et lorsqu'on voit que ça ne marche pas, on les contacte au niveau le plus élevé du DNS. Nous avons un processus opérationnel qui essaie de garantir la disponibilité et la résilience par rapport aux défaillances de la partie du serveur de noms de domaine. C'est comme ça que nous travaillons au niveau opérationnel.

Nous testons également ces systèmes pour être sûr que toutes les zones qui supportent le DNSSEC fonctionnent correctement, donc nous contrôlons l'intégrité au niveau du chiffrement au premier niveau.

AZIZ HILALI : Mon but est de donner la possibilité à tous ceux qui veulent poser une question, donc une minute pour la question et deux minutes pour la réponse, pas plus si on veut donner sa chance à tout le monde.

Donc j'ai Bakary, Ali, [Chonsselle ?], puis je verrai ce qui est écrit dans le chat, il y a des questions et des commentaires. D'abord, Bakary.

BAKARY KOUYATÉ : Merci. C'est Bakary, Internet Society, Mali.

En fait, moi j'ai des questions un peu orientées vers les utilisateurs finaux. On sait que parmi ces attaques, des organismes sont souvent ciblés mais le plus souvent les utilisateurs finaux paient le prix le plus fort. Est-ce que parmi les attaques certaines sont uniquement ciblées organismes ou bien utilisateurs finaux ? C'est ma première question.

Par rapport à ma deuxième question, la sécurité du nom de domaine ne relève pas de l'utilisateur final. Est-ce que pour moi, en tant qu'utilisateur final, si je trouve que mon domaine est attaqué par exemple, est-ce que j'ai la possibilité de porter plainte au niveau du bureau d'enregistrement ?

Merci.

AZIZ HILALI : Je vous propose qu'on prenne les trois questions et ensuite, vous répondrez.

La parole à Ali.

ALI AMESHAL : Bonjour. J'ai deux questions. Une précision de la part de Steve, d'abord. Le renouvèlement de nom de domaine, est-ce que nous avons cinq jours et est-ce que nous avons 30 jours ? Qui prend cette décision ? Est-ce que c'est le registre, le bureau

d'enregistrement ? Il semble qu'il y ait ici quelque chose qui n'est pas très clair parce qu'en général, d'après ce que je sais, il s'agit de 30 jours mais là j'entends parler de 5 jours. Quel est le délai ?

Ensuite, mon autre question, posée au monsieur avec une chemise jaune et assis à côté de Steve, vous, monsieur – David, oui. Vous avez parlé de gestionnaire de mots de passe et j'ai évité l'utilisation de gestionnaire de mots de passe parce que, dans mon cas, je soupçonne que si on met tous ses œufs dans le même panier, si quelqu'un veut usurper votre ordinateur, vous aurez laisser tous vos mots de passe entre les mains d'un même gestionnaire. Pourriez-vous éclaircir un peu cela ? Est-ce que j'ai raison ou bien est-ce vous qui avez raison ? Pourriez-vous répondre à cela ? Merci.

AZIZ HILALI : Allez-y.

INTERVENANT NON IDENTIFIÉ : J'ai deux questions. [Chancenne Bara ?], de la République du Congo. J'ai deux questions. La première question serait de savoir si l'ICANN a une procédure de résolution de litige ou encore des sanctions en cas d'attaques malveillantes d'un pays vers un autre.

La deuxième serait de savoir s'il y a une cellule de veille au niveau de l'ICANN qui fait l'étude des nouvelles applications mises en ligne pour avertir les utilisateurs des différentes failles que les acteurs peuvent utiliser pour les attaques malveillantes.

STEVE SHENG : Bien. Alors, je dois me rendre à une autre séance donc je vais répondre rapidement. Concernent le délai de grâce pour le renouvellement de nom de domaine, il y a un délai de 30 jours, un autre de 5 jours, je dois confirmer cela, ce sont deux choses différentes. Peut-être que Dave peut m'aider ici pour vous répondre, mais nous vous transmettrons cette information bientôt, pas de problèmes.

En ce qui concerne la responsabilité de l'utilisateur, je dirais que nous sommes tous responsables. D'un point de vue plus large, on veut assigner la personne qui peut régler le problème en général. Je pense que l'utilisateur joue un rôle important en ce sens parce que nous ne pouvons pas nous charger de tout, au niveau des registres et des bureaux d'enregistrement, leur demander de s'occuper de tout. Nous avons un rôle à jouer aussi. Les bureaux d'enregistrement et les registres ont aussi une responsabilité, bien sûr, mais je crois que tout le monde joue un rôle important ici pour lutter contre ces usurpations.

Nous devons assumer notre responsabilité et ensuite agir auprès de la personne qui peut régler le problème.

Ensuite, je ne peux pas répondre aux autres questions parce que je dois partir mais je crois que mes collègues ont mon adresse email, et Ariel, s'il vous plaît envoyez-moi les questions et je serai ravi d'y répondre par email. Merci.

DAVID PISCITELLO : Merci, Steve. Je vais rester un peu plus. Je vais donc essayer de répondre à vos questions, dans la mesure où j'arrive à m'en souvenir aussi.

Bien. Je vais reprendre ce dont Steve parlait au niveau de la responsabilité. Lorsque vous enregistrez un nom de domaine, c'est comme lorsque vous faites une location pour un appartement ou lorsque vous avez le permis de conduire. Vous avez la responsabilité de ce que vous allez faire avec ce nom de domaine et une chose que vous pouvez faire avec ce nom de domaine, c'est l'héberger, héberger des sites Internet, créer un serveur. Très souvent, vous allez choisir votre fournisseur de services Internet, parfois vous dépendrez d'une tierce partie, parfois vous allez héberger un opérateur local de site Web, et puis vous avez une autre partie, une tierce partie, qui va vous fournir des services. Donc vous êtes responsable du nom, et lui est responsable de l'exploitation du réseau. Très souvent, cela

diffère aussi du bureau d'enregistrement qui, à son tour, vous a donné un nom, et du registre. Donc le registre et le bureau d'enregistrement sont deux entités différentes.

Donc il y a beaucoup d'acteurs en jeu et jouent un rôle important, qui publieront des informations, enverront des emails. Si l'un d'entre eux est attaqué – une chose que je fais moi, je travaille au niveau de la sécurité – c'est d'essayer de comprendre d'où vient cette attaque, qui en est à l'origine, quel est l'acteur qui en est responsable et comment atténuer ce défi.

Ce n'est pas simple du tout, c'est une situation très compliquée avec beaucoup d'acteurs, qui parfois arrive même entre plusieurs juridictions. Le serveur se trouve en Hollande, l'attaquant est en Croatie et il y a quelqu'un qui envoie des bitcoins qui est en Amérique Latine, par exemple. Mon travail, dans ce cas-là, est très compliqué parce que je dois reconstruire une espèce de puzzle pour trouver le délinquant et l'arrêter. Bien sûr, l'ICANN travaille avec les forces de l'ordre pour arrêter ces délinquants. J'espère avoir répondu à votre question.

En ce qui concerne le délai de grâce de 5 jours ou de 30 jours, quel est le bon chiffre, en fait il y a en a plusieurs. La première période de grâce commence au moment où l'enregistrement de votre nom de domaine est conclus et dure 5 jours, afin de vous assurer que c'est bien le nom que vous vouliez, parce que

parfois les gens font des fautes de frappe lorsqu'ils enregistrent leur nom de domaine. Vous avez donc 5 jours pour corriger ces erreurs et dire « non, ce n'est pas ça mon nom de domaine » et ainsi vous ne perdrez pas votre argent. C'est comme un article échangeable dans un magasin avec le ticket de caisse.

Ensuite, si vous avez enregistré le nom de domaine pour plusieurs années et qu'au bout d'un an vous ne le renouvelez pas, vous avez 30 jours pendant lesquels le nom de domaine sera conservé jusqu'à ce que vous confirmiez l'enregistrement. Après l'expiration, vous avez 30 jours pendant lesquels le bureau d'enregistrement va attendre que vous confirmiez toujours vouloir ce nom de domaine, sinon vous le perdez. J'espère avoir répondu à votre question.

Ensuite, le gestionnaire de mots de passe. Le gestionnaire de mots de passe utilise un système de chiffrement solide. Sinon, je ne vous le conseillerai pas. Il faut qu'il y ait un chiffrement des informations, sinon ça ne sert à rien. La plupart des gestionnaires de mots de passe utilise des systèmes de chiffrement très solides, ce n'est pas quelque chose de facile à pirater. La valeur de ce gestionnaire de mots de passe, c'est que vous pouvez créer un mot de passe très solide et le gestionnaire de mots de passe vous génèrera ces mots de passe, vous n'avez pas à vous en souvenir. Vous aurez votre mot de passe qui apparaîtra automatiquement sur le site sur lequel vous vous

rendez. Ce que je fais c'est que je leur demande des mots de passe de 24 caractères et ce gestionnaire me les donne. À chaque fois que je vais sur un site Internet, le mot de passe est rempli pour moi et je n'ai pas besoin de m'en souvenir. Je trouve ça très utile, personnellement.

Alors, les attaques entre pays, maintenant. L'ICANN n'est pas un organisme gouvernemental. Nous ne participons pas aux réunions des Nations Unies ou du Conseil de l'Europe, nous ne sommes qu'observateurs, nous ne participons pas aux interactions entre gouvernements. Notre seule interaction avec des gouvernements vise à encourager un Internet ouvert, encourager le maintien d'un DNS ouvert et unifié. Nous soutenons les gouvernements dans leurs opérations de services liés aux noms de domaine. Nous ne sommes pas une organisation politique dans ce domaine-là au niveau de sanctions que nous pourrions imposer à des gouvernements en infraction avec certaines règles.

Ensuite, au niveau des fonctions, nous ne sommes pas des développeurs de logiciel. Si vous voulez par exemple acheter une application sur l'ITunes Store ou ailleurs, nous n'avons rien à voir avec tout ça. Nous ne développons pas d'application. Parfois, certaines choses ont l'air d'affecter le DNS, alors nous savons que cela existe, nous connaissons la vulnérabilité qu'une application peut causer. À ce moment-là, nous allons écrire un

avertissement sur notre site Internet à ce propos, mais cela ne fait pas partie de notre activité.

Est-ce que j'ai répondu à tout ? On me pose des questions, j'essaie d'y répondre. Je sais que je dois être rapide, mais il me faut y répondre.

AZIZ HILALI : Le fait que nous ayons beaucoup de questions d'intervenants montre que la séance a été vraiment intéressante.

Steve et David, nous vous remercions pour cette conférence.

Je m'adresse aux ALS, si cela vous intéresse, on peut très bien organiser un webinaire en ligne pour pouvoir continuer un peu cette discussion très intéressante. J'ai l'impression que cela intéresse beaucoup les ALS.

On doit finir parce qu'on doit libérer la salle pour l'ALAC, pour nous et pour l'ALAC et aussi donner 5 minutes pour les interprètes que je remercie et que je ne remercierai jamais assez.

Tu veux dire un petit mot, Tijani ?

TIJANI BEN JEMAA : Oui, merci, je vais le dire en français.

Dans le cadre du programme de renforcement de capacités de l'ALAC, nous avions déjà fait un webinaire sur ce même sujet, avec Steve d'ailleurs, et ça a été bien suivi. Aujourd'hui, je vois qu'il y a beaucoup d'intérêt donc si vous souhaitez qu'on fasse un autre webinaire, on est prêts à le faire. Juste exprimez votre besoin parce qu'on ne veut pas faire un webinaire et se retrouver avec seulement deux ou trois personnes.

AZIZ HILALI : Tijani me dit de dire un petit mot de clôture. Merci beaucoup et donc on vous donne rendez-vous pour [inaudible]. Je remercie Dave et Steve une nouvelle fois, et les interprètes, le personnel, tout le monde, voilà. Merci beaucoup et rendez-vous tout à l'heure.

[FIN DE LA TRANSCRIPTION]