YEŞIM NAZLAR : Bonjour, bon après-midi et bonsoir à tous. Soyez les bienvenus au cinquième webinaire des cinq webinaires obligatoires d'ATLAS III. Aujourd'hui, nous allons faire une introduction à la cybersécurité. Notre présentateur aujourd'hui est Patrick Jones, directeur sénior de l'engagement des parties prenantes au niveau global.

Nous n'allons pas faire d'appel nominal pour cet appel. Toutefois, nous allons prendre en considération votre participation dans les dix premières minutes de cet appel. Après quoi, votre participation ne sera plus prise en considération comme critère pour ATLAS III. Si vous êtes connecté uniquement sur le phone bridge, veuillez s'il vous plaît rejoindre Zoom étant donné qu'il s'agit là d'un critère obligatoire pour la prise en compte de votre participation.

Nous avons de l'interprétation en espagnol et français pour ce webinaire. Petit rappel, veuillez indiquer votre nom avant de prendre la parole afin de permettre aux interprètes de vous identifier sur les autres canaux ainsi que pour la transcription. Veuillez également parler à un rythme raisonnable afin de permettre aux interprètes de faire un bon travail.

Toutes les lignes seront sur muet pendant la présentation puis ouvertes pour la séance de questions et réponses à la fin de la présentation.

Vous aurez remarqué que nous organisons ce webinaire sur la plateforme Zoom dont les caractéristiques ressemblent à celles d'Adobe Connect. Afin de voir la liste des participants et d'avoir accès au chat,

veuillez cliquer sur l'icône en bas de l'écran. Vous ne pourrez voir les échanges sur le chat qu'à partir du moment où vous rejoignez l'appel et non pas avant. Pour lever la main, il suffit de cliquer sur l'icône « Lever la main. »

Je vais maintenant céder la parole à Joanna Kulesza, coprésidente du sous-groupe de travail sur le renforcement des capacités pour ATLAS III. Joanna, c'est à vous. Merci.

JOANNA KULESZA : Merci beaucoup Yeşim, merci de cette introduction. Merci à tous ceux qui nous ont rejoint aujourd'hui pour cet appel, le cinquième de cette série de webinaires obligatoires pour ATLAS III. Merci beaucoup Patrick d'avoir pris le temps de nous faire cette introduction aujourd'hui à la cybersécurité. Nous avons eu la première version de ce webinaire hier avec votre collègue David, qui nous a donné un aperçu de la cybersécurité. J'ai particulièrement apprécié que Patrick fasse cette présentation aujourd'hui étant donné son parcours dans le domaine de la cybersécurité, de la confidentialité et des organisations internationales. Donc j'attends avec impatience d'entendre la présentation de Patrick.

C'est à vous Patrick. Si vous parlez, Patrick, on ne vous entend pas sur la ligne.

PATRICK JONES : Me revoici, je suis là. Excusez-moi, l'internet a crashé juste au moment où j'allais intervenir. Ça y est ? Je peux commencer ?

JOANNA KULESZA : Oui, l'enregistrement est commencé. Je viens de conclure l'introduction et je vous cédais la parole. On est maintenant prêts.

PATRICK JONES : Merci. Merci beaucoup de m'avoir invité pour faire ce webinaire. Pour ceux qui ont suivi le webinaire d'hier soir, vous aurez entendu David Huberman de notre équipe du CTO. Moi, je suis Patrick Jones de l'équipe engagement des parties prenantes au niveau mondial. Cela fait 13 ans que je travaille à l'ICANN. Et avant de rejoindre l'équipe à laquelle j'appartiens maintenant, je travaillais à la CTO également pendant six ans.

J'espère que cette présentation va vous paraître utile pour compléter les outils qui sont disponibles sur ICANN Learn. Nous avons récemment ajouté un cours sur une introduction à la cybersécurité, les utilisations malveillantes du DNS aussi. Donc j'espère que cela va vous sembler utile pour avoir plus d'informations et de renseignements sur ce sujet. Sur ce, nous allons avancer sur cette présentation. Diapositive suivante s'il vous plaît.

Nous allons commencer en vous donnant un aperçu des éléments essentiels qui figurent dans tout type de réseau. Cela peut figurer dans un réseau d'une entreprise, d'une université, d'un gouvernement. Donc typiquement, il y a des serveurs courriels dans ces réseaux qui fournissent des courriels, des fonctions de calendrier, des informations relatives aux contacts. Ensuite, il y a des serveurs de base de données qui peuvent contenir des données relatives aux biens, aux clients ou

d’autres types d’informations stockées par les organisations gouvernementales ou internationales et ensuite des informations financières liées à un gouvernement, une entreprise, une organisation ou des processus et procédures liées à l’organisation. Tout cela dépend du type d’organisation en question. Diapositive suivante s'il vous plaît.

Donc parce que toutes les organisations ont ces éléments, ce sont des cibles attrayantes pour des attaques. Ces fonctions remplissent un certain nombre de fonctions, d’abord la gestion d’identité qui inclut les identifiants et les mots de passe comme les mesures biométriques, l’authentification. Et cela peut également être la gestion des clés cryptographiques.

Le stockage de données, c’est ce qu’on fait lorsqu’on stock des données. C’est également la durée de stockage de ces données. Et il peut y avoir des politiques par rapport aux pratiques liées à la sécurité pour gérer ces informations sur le réseau. Il y aura des systèmes qui seront mis en place, hardware, software, le patch aussi.

Et si votre organisation est connectée à l’internet, la plupart le sont, vous aurez des adresses IP qui vont connecter leur réseau par l'intermédiaire du DNS à l'internet. Et chaque jour, tout cela fait l’objet d’attaques, attaques vis-à-vis du système dont l’objectif est d’extraire des données. Diapositive suivante s'il vous plaît.

Donc lorsqu’on parle du type de cybercriminalité, sachez qu’il y a notamment le hameçonnage qui consiste à envoyer des courriels qui sont supposés provenir d’une organisation, d’une entreprise, bref quelqu'un en qui vous avez confiance, afin de tromper le destinataire et de l’inciter à révéler des informations, que ce soit le mot de passe, les

numéros de carte bancaire, l'identifiant qui permet ainsi à l'auteur du délit d'avoir accès à un courriel ou à d'autre type d'informations. C'est très commun.

Autre type de délits dans le domaine de la cybercriminalité, c'est un logiciel malveillant. C'est un logiciel qui est créé pour perturber, endommager et obtenir un accès non autorisé à un système informatique. Cela inclut par exemple les rançons logiciel ; votre machine est bloquée et pour avoir accès à votre ordinateur, l'auteur de l'attaque vous dit : « Il faut payer une rançon et on vous rendra l'accès à votre ordinateur. » Cela, c'est toujours très dangereux.

Autre exemple de cybercriminalité, ce sont les réseaux zombies. C'est un réseau d'ordinateurs privés qui sont connectés entre eux et qui contrôlent en tant que groupe et qui infectent votre ordinateur avec un logiciel malveillant. Il y a des réseaux zombies qui sont contrôlés par des noms de domaine qui sont contrôlés à distance. Mais je vais en parler dans un instant. Diapositive suivante s'il vous plaît.

À l'ICANN, vous aurez certainement entendu parler de l'utilisation abusive ou malveillante du DNS. Si vous ne savez pas ce que c'est, en fait, ce sont des individus, des entreprises qui utilisent le système des noms de domaine pour résoudre leur nom et les lier à des adresses de protocole internet. C'est parce que les adresses IP qui sont basées sur des numéros sont difficiles à retenir pour l'être humain. Mai si vous pouvez lier un nom à un numéro, alors c'est plus facile de s'en souvenir et d'utiliser le système des noms de domaine et d'envoyer des requêtes sur votre ordinateur.

Maintenant, les personnes qui sont à l'origine de ces abus essaient de perturber, de déstabiliser ce système des noms de domaine à d'autres fins. Et ils peuvent le faire en perturbant des transactions commerciales par exemple sur des sites web de banques, des sites d'organisations gouvernementales ou sur les réseaux sociaux.

On voit aussi des organisations qui font l'objet de ces attaques et qui sont trompées. Ces attaques se font par des noms de domaine enregistrés de manière malicieuse ou des services d'enregistrement ou résolution de noms qui sont piratés.

Je vais vous parler de quelques exemples d'attaques cybernétiques courantes. Certaines de ces attaques visent le système internet, le système de courriels et également une atteinte à modifier la résolution de noms. Cela, c'est une utilisation malveillante du DNS. Et je vais vous parler d'un exemple concret qui a eu lieu en avril 2018.

Vous voyez ici un exemple. Le domaine en question, c'était myetherwallet.com. C'est un domaine qui a été utilisé pour héberger de la cryptomonnaie et ce domaine a fait l'objet d'une attaque. Les auteurs de l'attaque ont utilisé ce domaine pour rediriger les utilisateurs vers un domaine faux. Et une fois que les utilisateurs se connectaient sur le domaine faux, alors ils donnaient leur identifiant et les auteurs de cette attaque volaient leur identifiant et la cryptomonnaie qu'ils y déposaient.

L'argent qui a été volé s'élève à 21 millions $ en cryptomonnaie et cela n'est qu'un exemple parmi tant d'autres où le piratage a donné lieu à une perte d'informations, d'identifiants et d'argent surtout des utilisateurs.

Deuxième exemple, parfois, les attaques cybernétiques sont motivées par des raisons politiques. En novembre de cette année – et cela a parfois encore lieu, – il y a eu quelques attaques très bien coordonnées qui sont connues comme DNSpionage et la campagne Sea Turtle. Cela, c'est un exemple qu'on a appelé prépositionnement d'attaques cybernétiques militaires. Il s'agit de collecter tous les renseignements qui sont nécessaires pour lancer des attaques cybernétiques militaires.

Les chercheurs ont identifié qu'il y avait 40 organisations impliquées dans 13 pays. En fait, il y en avait beaucoup plus mais dans l'attaque initiale qui a eu lieu, les pays concernés se trouvaient en Afrique du Nord, au Moyen-Orient, les sites gouvernementaux et les entreprises y compris certaines compagnies aériennes. On a ciblé également des entreprises pétrolières, des fournisseurs de DNS qui sont bien connus en Suède et dans d'autres pays d'Europe qui ont également fait l'objet d'attaques et une grande entreprise de courrier postal aux États-Unis. Ils ont également pu infiltrer les courriels DNS et les autorités et obtenir des documents [cryptés]. Diapositive suivante s'il vous plaît.

Alors, le rôle de l'ICANN est assez limité. Des choses que nous pouvons faire, c'est de fournir une plateforme qui permet de partager les expériences et de sensibiliser sur les problèmes. Lors de la dernière réunion de Kobe au Japon, au sein du comité consultatif sur la sécurité et la stabilité, certains ateliers ont été organisés avec des directives pratiques pour les différents acteurs qui participaient pour les guider de manière à mieux protéger les réseaux, donc pour toute personne qui a un nom de domaine. Je vous donnerai des exemples par la suite mais les attaques qui se produisent ont un impact sur tout le monde, depuis les

gouvernements, aux sociétés, aux agences d'application de la loi et aux utilisateurs finaux de l'internet d'une manière générale.

Nous avons l'équipe technique de l'ICANN du bureau technique qui travaille avec les membres de la communauté et l'organisation ICANN pour partager des informations pour sensibiliser, définir ce qui peut être fait et pour fournir une plateforme de partage des informations en cas d'attaque relative à la sécurité.

Alors ensuite, un petit historique sur le rôle de l'ICANN. Avant qu'un incident se produise, dans le cadre des statuts, il y a un accent qui est mis sur le fait qu'il faut s'assurer que le système d'identificateurs uniques de l'internet est stable et sécurisé puisque ceci est au cœur de notre travail. Il y a également des engagements dans les statuts, donc préserver et améliorer l'administration du DNS et la stabilité, la fiabilité et la sécurité opérationnelle ainsi que l'interopérabilité mondiale, la résilience et l'ouverture du DNS et de l'internet.

Les moyens que nous avons pour y arriver sont de fournir des moyens pour les parties contractantes, les opérateurs de registre et les bureaux d'enregistrement, de partager les informations lorsqu'il y a des vulnérabilités, lorsqu'il y a des attaques. Nous avons également des plateformes qui permettent lors des réunions de communiquer, il y a des listes de diffusion qui permettent de communiquer là-dessus de manière à mieux comprendre les menaces sur la sécurité. Nous travaillons également avec d'autres partenaires dans l'écosystème de l'internet, y compris les RIR, les organisations de noms de domaine de premier niveau. Donc nous travaillons de manière collaborative pour faire part aux uns et aux autres de nos expériences mutuelles.

À l'ICANN, il y a des termes qui sont utilisés fréquemment, donc on parle de sécurité, de stabilité et de résilience. Alors qu'est-ce que cela veut dire ? La sécurité, c'est la capacité à protéger et à éviter la mauvaise utilisation des utilisateurs uniques de l'internet. La stabilité fait référence à la capacité à s'assurer que le système fonctionne comme il doit fonctionner et donc s'assurer que les utilisateurs des identificateurs uniques ont confiance en la manière dont le système fonctionne. Résilience, c'est la capacité pour le système d'identificateurs uniques de résister aux attaques malveillantes et à d'autres problèmes d'interruption de service.

Il y a un certain nombre d'engagements en matière de sécurité, de stabilité et de résilience du système d'identificateurs uniques. Nous travaillons en encourageant tous les acteurs de l'internet à participer activement à l'élaboration des politiques. Il y a également le travail technique.

Je vois les commentaires dans le chat de Zoom. Donc je crois effectivement que l'équipe At-Large vous enverra les diapositives à la fin de la séance. J'espère que cela répond à la question qui a été affichée.

Nos engagements sont également de travailler de manière collaborative avec les acteurs régionaux de manière à fournir des formations sur la sécurité, des formations sur le DNS et autres moyens de renforcer les capacités. Très souvent, ceci est basé sur les demandes des organismes locaux. De temps à autre, il y aura une formation sur les extensions sécurité du DNS ou alors nous aurons des formations sur les abus du DNS, comment les reconnaître et comment réagir. Cela dépend un petit

peu de l'intérêt au niveau régional et des demandes qui nous arrivent en matière de formation. Diapositive suivante.

Au sein des différents groupes de parties prenantes et des organisations de soutien aux comités consultatifs, il y a différents groupes qui soutiennent le SSR.

Le premier groupe dont j'aimerais parler est au sein du GAC et il s'agit du groupe de travail sur la sécurité publique. Ce groupe existe depuis je crois six ou sept ans. Et à la base, l'idée était de rassembler les organisations de sécurité publique et les agences d'application de la loi, les acteurs d'application de la loi. Ce groupe a fourni un certain feedback lors des commentaires publics, tout ce qui est relatif à l'abus de DNS. Le travail a permis d'améliorer les différents contrats que nous avons avec les parties contractantes. Ce groupe a également permis de communiquer avec le GAC sur les questions de sécurité.

Il y a deux autres groupes qui se concentrent sur ces questions de sécurité, de stabilité et de résilience. Il s'agit d'abord du comité consultatif sur la stabilité et la sécurité de l'ICANN. Il s'agit d'un comité consultatif entre le Conseil et la communauté qui évalue les menaces, qui analyse les risques du système d'identificateurs uniques. Souvent, il y a des séances publiques qui sont organisées par ce groupe au sein des réunions de l'ICANN. Les thèmes discutés sont les attaques des IDN. Il y a également tout ce qui est relatif aux différentes attaques. Le SSAC aura des séances lors des réunions suivantes sur l'internet des objets qui seront intéressantes.

Et enfin, le RSSAC, comité consultatif sur le système des serveurs racine, il conseille le Conseil d'Administration et la communauté sur des

questions relatives au fonctionnement, à l'administration, à la sécurité, à l'intégrité du système de serveurs racine. Nous en parlerons davantage lors des réunions à venir mais au Maroc en tout cas, je crois qu'il y aura une opportunité de commenter sur la proposition de modèle de gouvernance du RSSAC. Donc il y aura davantage de travail là-dessus et davantage d'opportunités de feedback de la part de la communauté dans ce domaine. Diapositive suivante.

Nos relations entre les parties contractantes, opérateurs de registre et bureaux d'enregistrement sont vraiment des outils clés pour promouvoir la sécurité, la stabilité et la résilience. Le contrat d'accréditation de bureaux d'enregistrement impose un devoir d'investiguer, de faire des enquêtes sur les abus, d'utiliser les preuves d'abus par rapport aux noms de domaine qui sont gérés par ces bureaux d'enregistrement. Et dans le contrat de registre, il existe une disposition qui interdit aux détenteurs de noms de domaine de diffuser ou de distribuer les programmes malveillants, d'avoir des réseaux zombies, de faire du hameçonnage, etc. Diapositive suivante.

Vous avez là un petit dessin qui vous explique un petit peu comment les parties contractantes sont reliées dans l'écosystème de l'internet. Nous avons un lien direct entre l'ICANN et les opérateurs de registre au premier niveau qui est géré les contrats d'enregistrement. Vous avez également le RAA entre l'ICANN et les bureaux d'enregistrement.

Il y a des contrats également entre opérateurs de registre et bureaux d'enregistrement, ceux qui exploitent le nom et ceux qui le proposent. De temps à autre, les bureaux d'enregistrement utilisent des revendeurs mais ces revendeurs n'ont pas de contrat avec l'ICANN. Donc il y a

souvent des questions dans la communauté sur les questions qui sont soulevées au niveau des revendeurs. Mais en fait, c'est quelque chose qui est en dehors de la relation avec l'ICANN.

Les bureaux d'enregistrement et les revendeurs ont une relation avec le titulaire du nom de domaine. Il s'agit donc du contrat du titulaire de nom de domaine, *registrant agreement*. Ces contrats sont disponibles sur le site de l'ICANN. Il y a une page sur le site de l'ICANN également par rapport au RAA. Vous pouvez voir tout ceci sur notre site web. Et si travaillez avec un bureau d'enregistrement et si vous voulez savoir quelles sont vos attentes, vous pouvez vous rendre sur le site web de votre bureau d'enregistrement. Vous pouvez également envoyer une note au département de conformité de l'ICANN si vous avez des questions par rapport à cela. Diapositive suivante.

Il y a une filiale de l'ICANN qui s'appelle la PTI, identificateurs techniques publics, qui s'occupe des aspects opérationnels de coordination du système d'identificateurs uniques de l'internet. La PTI attribue les ressources en numéros, que ce soit les adresses IPv4, IPv6 ou les numéros de système autonome au RIR. La PTI s'occupe également d'entretenir la zone racine, administre la zone ARPA. Et par ailleurs, l'ICANN par la PTI entretient la chaîne de confiance pour les DNSSEC et coordonne plus de 3 000 opérateurs de registre pour les protocoles de l'IETF. Ceci nous amène à fournir davantage de contexte en fait par rapport aux DNSSEC justement. Donc passons à la diapositive suivante.

Lorsque la communauté technique de l'internet et les spécialistes ont mis au point le DNS, en fait la sécurité n'était pas quelque chose de très

important. On ne s'en préoccupait pas beaucoup. À l'époque, il y avait un certain nombre de vulnérabilités qui ont été découvertes. Et comme réponse à ces problèmes, la communauté technique, les experts ont découvert un nouveau protocole qui s'appelait les DNSSEC. L'idée, c'était d'ajouter un autre niveau de sécurité et de protection aux données DNS.

Un certain nombre d'opérateurs d'extensions géographiques ont joué un rôle de chef de file à cette époque-là et à l'ICANN, on a commencé à lancer le DNSSEC pour s'assurer qu'il y a authentification, vérification et cela a fourni également une chaîne de confiance depuis le niveau le plus haut du système du DNS jusqu'au niveau des opérateurs de registre individuels, donc la zone racine et les extensions telle que .com. Puis lorsque les banques, les compagnies aériennes, les autres organisations mettent en œuvre le DNSSEC, cela permet aux opérateurs de DNS de valider que toutes les données qui passent par eux sont valides et que l'utilisateur ne peut pas être réorienté de manière malicieuse vers d'autres domaines faux. Diapositive suivante s'il vous plaît.

Le DNSSEC se fonde sur les technologies de PKI, infrastructure de gestion des clés publiques. Il s'agit des clés cryptographiques qui sont tout en haut de la hiérarchie. Il s'agit d'une partie publique. C'est le point de départ de confiance pour la validation que les résolveurs utilisent. Et la partie privée concerne la clé de signature de zone. Cette clé de signature de zone, elle concerne le niveau le plus élevé et les opérateurs de registre individuels, eux, s'occupent de la zone dont ils sont responsables. Et cela constitue une chaîne de confiance qui fournit un plus haut niveau de sécurité pour le système du DNS. Diapositive suivante s'il vous plaît.

Je vous le disais, les PTI, identificateurs techniques publics, ont la fonction d'émettre, de gérer, de changer et de distribuer les clés du DNS. Ils signent les ensembles de clés et plusieurs fois par an, nous organisons des cérémonies de clés. Quiconque peut les suivre à distance, c'est quelque chose de public, ainsi que les dernières actualités sur la KSK, les signatures de clés. En général, tout cela est publié longtemps à l'avance pour annoncer la tenue de ce type de cérémonie sur le site web de l'ICANN et c'est une excellente manière très intéressante du reste de voir comment est-ce que les identificateurs techniques publics sont sécurisés. Diapositive suivante s'il vous plaît.

L'équipe CTO ainsi que différentes équipes chargées de l'engagement travaillent avec des membres de la communauté sur des questions liées à la sécurité cybernétique, sécurité des identificateurs. On organise des webinaires, des réunions lors des conférences ICANN, des ateliers, des formations, donc toute une série d'activités liées au renforcement de capacités. Il y a deux semaines, bon nombre d'entre nous ont participé à des séances sur un colloque sur le DNS à Bangkok. Et il y avait d'autres ateliers dont un sur le renforcement de capacités qui a eu lieu avec THNIC avec les opérateurs de registre de Taïwan. Et pendant toute l'année, dans beaucoup de pays du monde, l'ICANN participe à des activités de renforcement de capacités afin de partager nos connaissances, notre expérience avec d'autres acteurs dans ce domaine. Diapositive suivante s'il vous plaît.

Lorsqu'un incident en termes de cybersécurité se produit, l'ICANN a un rôle à jouer. Mais voyons également ce que font les différentes organisations. L'ICANN fait partie d'abord de l'équipe de réponse en cas

d'incident et d'autres équipes au niveau national font également partie de cette plateforme pour partager des informations lorsqu'il y a ce genre d'attaques. Ils partagent en général ce genre d'informations avec d'autres opérateurs de registre, autorités de sécurité publique, que ce soit les autorités chargées de l'application de la loi, INTERPOL, Europol et les autorités internationales. Également, cela inclut une réponse coordonnée entre les bureaux d'enregistrement et les opérateurs de registre des domaines de premier niveau. Ce sont des personnes qui sont impliquées dans l'atténuation des attaques cybernétiques ou dans le fait d'apporter une réponse coordonnée à ces attaques.

Lorsque ce genre d'attaque se produit, il est très difficile d'identifier la source de cette attaque. Il n'en demeure pas moins qu'il est important qu'on essaie d'identifier les adresses de protocole internet qui sont utilisées, s'il y a des noms de domaine qui sont impliqués dans cette attaque, voir où se situent les bureaux d'enregistrement et opérateurs de registre de ces noms de domaine. Et ensuite, les organisations peuvent vérifier leur base de données pour voir s'ils peuvent nous aider à identifier d'où provient la source ou l'origine de l'attaque. Ensuite, il faut donner d'autres sources de données qui peuvent inclure les données d'enregistrement associées aux adresses IP et numéros AS.

Comme je l'ai dit auparavant, à l'ICANN, il y a une équipe au sein de notre bureau de la CTO et on travaille avec d'autres organisations pour apporter une réponse coordonnée à ces attaques. Cette équipe fournit une compréhension très approfondie par rapport à ce qui se produit, quel genre de réponse il faut apporter lorsqu'une attaque se produit. Et l'équipe participe avec les organisations chargées de l'application de la loi, les opérateurs de registre, les bureaux d'enregistrement. Ils font un

historique pour partager leur expérience une fois que cette attaque a eu lieu. Et nous indiquons sur notre site web des informations pour aider les autres à se montrer moins vulnérables à ce genre d'attaques.

Et il y a quelques temps maintenant, lorsqu'un membre de la communauté de l'ICANN a découvert une vulnérabilité dans le système d'Adobe Connect auquel on se connectait pendant les réunions sur la zone racine – on est passés maintenant à la plateforme actuelle Zoom –, on a pu le faire grâce à la réponse rapide de ce membre de la communauté qui a indiqué qu'il avait identifié cette vulnérabilité ; il nous l'a fait savoir. Donc cela, c'est un exemple de la manière dont on travaille de manière coordonnée avec les autres. Nous avons pris cette information, on l'a fait connaître à Adobe et Adobe a ensuite pu ajuster son réseau avec ces informations.

Diapositive suivante : quelle est le rôle de l'ICANN après un incident cybernétique ? On partage nos expériences à l'occasion des colloques de l'ICANN sur le DNS, également avec la communauté OARC, le centre de recherche [inintelligible] opérations du DNS et avec les groupes d'opérateurs de réseau. Et on peut tous récupérer cette information, la partager sur nos réseaux, voir si on a besoin de nouvelles politiques, de modifier certains termes de nos contrats ou peut-être identifier des protocoles qui doivent être améliorés ou développés davantage. Et ce qu'on peut faire aussi, c'est partager ces opérations avec les groupes d'opérateurs de réseau, agences d'application de la loi, etc.

Nous nous acheminons vers la fin de cette présentation. Avant de passer aux questions, une petite conclusion avec les principaux enseignements de cette présentation.

Le DNS, ce n'est plus simplement une fonction technique qui est gérée par les administrateurs de système, mais c'est une infrastructure critique qui est utilisée dans nos communications journalières, que ce soit les courriels, la navigation sur le web, les applications mobiles. Et c'est une plateforme vers d'autres choses comme les dispositifs, tous les dispositifs qui sont liés à l'internet comme les frigos par exemple. C'est pourquoi il est fondamental que les décideurs politiques et les organisations soient conscients de cette infrastructure du DNS. Si cette infrastructure est en danger, alors c'est tout le système et les réseaux qui sont en danger.

Quelques recommandations faites par l'ICANN au début de cette année. L'ICANN et d'autres organisations ont publié ces recommandations pour la communauté de l'internet dans son ensemble. Il s'agit de choses qu'on peut faire comme par exemple mettre en œuvre et reconnaître les meilleures pratiques pour renforcer les réseaux, authentification des systèmes, encryptement, vérifier que vous avez un système de courriels vigoureux. Vous pouvez voir ici un lien en bas de la page. L'une des recommandations importantes, c'est de permettre la mise en œuvre du DNSSEC parce que cela permet d'atténuer l'impact des attaques. Diapositive suivante s'il vous plaît.

La sécurité, la stabilité et la résilience, c'est un domaine prioritaire pour l'ICANN. Donc pour la communauté de l'ICANN dans le domaine de la cybersécurité, il y a le hameçonnage, le logiciel malveillant, les rançons logiciel, les réseaux zombies, etc. mais également les pratiques commerciales frauduleuses et trompeuses. Et la communauté fait beaucoup d'efforts pour contribuer à accroître la stabilité, la sécurité et la résilience de l'internet.

Sur ce, je suis à votre disposition si vous avez des questions. J'espère qu'il y en a. Et je ferai de mon mieux pour vous apporter des réponses.

Alors je vois qu'il y a quelques questions sur le chat Zoom.

Les attaques de déni de service peuvent faire tomber les réseaux internet, y compris les noms de domaine d'hébergement de serveur. Donc les attaques de déni de service, c'est un type d'attaque. Je ne veux pas trop rentrer dans le détail des différents types d'attaques qu'on peut observer. En fait, j'ai essayé de me concentrer sur un contenu de fond et de rester à haut niveau.

JOANNA KULESZA : Patrick, si vous le permettez, on a une question de Joan qui souhaite poser sa question. Joan, est-ce que vous êtes avec nous ? Vous pouvez poser votre question, Joan. Non, ce n'est pas le cas.

Est-ce qu'il y a d'autres questions de la part des participants ? Allez-y, levez la main, n'hésitez pas. Je vais commencer par les questions qu'on a eues hier. J'espère que cela pourrait être utile pour les autres.

David nous adonné quelques points de vue, mais par rapport à ce que peuvent faire les utilisateurs finaux de manière générale pour mieux comprendre ou pour mieux gérer leur sécurité, j'ai trouvé que cette question était utile par la communauté. Elle a été posée hier. J'aimerais savoir si vous avez des commentaires à nous donner là-dessus.

PATRICK JONES : Je n'ai pas en fait entendu la présentation d'hier faite par David, donc par exemple que ma réponse sera un petit peu différente de la sienne.

Mais en tant qu'utilisateur final, une des premières choses que vous pouvez faire, si vous avez par exemple un nom de domaine et que vous êtes passé par un bureau d'enregistrement, c'est de demander à votre bureau s'il propose les DNSSEC, donc les extensions de sécurité du système des noms de domaine, donc de suggérer d'ajouter ceci au service que vous obtenez de votre bureau d'enregistrement.

Vous pouvez également employer une sécurité pour votre courriel. Vous pouvez essayer de ne pas réutiliser vos mots de passe sur les différents sites sur lesquels vous appuyez. Vous pouvez également essayer de connaître qui a accès à vos domaines critiques, à vos services critiques, donc qui a accès aux courriels pour la société ou pour l'agence gouvernementale dont vous êtes responsable. Les bases de données clés que vous utilisez, qui y a accès ? Ou alors si vous êtes un utilisateur de base et que vous n'avez pas votre propre nom de domaine mais que vous utilisez un système bancaire en ligne, faites attention au lieu où vous utilisez votre mot de passe pour avoir accès à votre banque ou à votre courriel. Essayez aussi d'utiliser une authentification multifacteur, à deux facteurs ou à multiple facteurs. Donc c'est par cela que je commencerais. Et j'espère que cela sera utile, ces petits conseils.

JOANNA KULESZA : Merci Patrick.

Nous avons quelques questions dans le chat. J'espère que vous les voyez. Sinon, dites-moi, je peux vous les lire.

PATRICK JONES : La question de Satish : « Comment est-ce que le DNS va évoluer à l'avenir ? Il y a d'autres personnes qui pensent que d'autres ressources sont disponibles en ligne.» Il faut savoir que ces applications s'appuient sur certains noms pour se connecter par l'application à des machines qui sont au sein de l'application.

Donc le DNS, c'est toujours une technologie clé sous-jacente. On l'utilise de plus en plus au fur et à mesure que différents dispositifs sont connectés au DNS. Donc du point de vue de l'ICANN, nous ne prévoyons pas une diminution de l'importance du DNS. Il y aura peut-être d'autres manières, d'autres méthodes d'exploitation du DNS mais c'est quand même une infrastructure sous-jacente majeure. Et lors des réunions que nous avons, nous présentons des séances telles que la journée Tech, des sessions de travail, d'autres séances sur l'évolution du DNS. Et nous les organisons avec le Conseil d'Administration, les groupes d'experts techniques qui souvent vont parler des évolutions techniques du DNS. Et ces séances sont de bonnes séances à mon avis à suivre et à observer pour mieux comprendre.

Question de Michael sur la gouvernance : « Il semble que c'est nécessaire pour la cybersécurité. Quelles sont les démarches qui permettent de réussir ? »

Alors une des choses que nous faisons dans on équipe, l'équipe d'engagement des acteurs mondiaux, c'est d'encourager la participation au niveau technique au sein de l'ICANN. Et si cela vous intéresse, les questions des sécurité du DNS, lors des réunions, il y a différentes manières d'être impliqué : participer aux réunions techniques ou suivre à distance, il y a différents groupes qui participent et il y a différents

groupes qui vraiment s'appuient sur les bénévoles. Donc si la cybersécurité et les questions techniques vous intéressent, essayez de participer aux efforts de l'ICANN ou aux efforts de nos partenaires pour voir un petit peu quels sont les sujets clés dont on parle et ce qui vous intéresse en particulier.

JOANNA KULESZA : Nous avons une autre question de Michael focalisée sur le financement, le soutien pour les pays de l'hémisphère Sud. Et je crois que Joan également a une question à poser.

Celle de Michael est dans le chat.

PATRICK JONE : Alors est-ce qu'on pourrait remonter dans le chat ? Voyons... Alors, les efforts en matière de développement, nous en parlons souvent dans des forums tel que...

JOANNA KULESZA : Désolé, apparemment il y a eu un problème de connexion. Nous avons perdu Patrick. Nous ne vous entendons pas, Patrick. Nous avons perdu Patrick, désolée. Donc nous allons le reconnecter. Nous allons simplement vous demander de patienter un petit instant s'il vous plaît.

Nous avons la question de Michael. Dès que Patrick sera de retour, nous lui demanderons de répondre à cette question. Ensuite, il y a deux mains levées d'Abdalmonem Galila. Donc lorsque Patrick sera de retour, nous passerons la parole à ces personnes. Et il y a deux autres questions qui ont été envoyées dans le chat et j'espère que nous aurons le temps

de répondre à toutes les questions. En ce qui concerne les questions techniques, nous verrons ce que nous pouvons faire. Peut-être que nous allons dépasser un petit peu le temps imparti.

Encore une fois, désolée pour cette petite interruption technique. J'espère que nous allons pouvoir trouver une solution dans les quelques minutes à venir.

Merci Glenn d'avoir géré le chat. Vous voyez qu'il y a eu conversion des diapositives en livre eBook. Donc j'apprécie beaucoup, merci.

Yeşim, est-ce qu'on a rappelé Patrick ? Que se passe-t-il ?

YEŞIM NAZLAR : Joanna, nous sommes en train d'essayer de joindre Patrick par Skype. Son problème, c'est qu'il n'a pas d'internet. Il y avait un problème d'internet de nouveau. Désolée encore une fois de ce retard. Je fais ce que je peux.

JOANNA KULESZA : Merci beaucoup. Ce serait bien d'avoir l'audio, que ce soit par téléphone ou par Zoom. Donc voilà, merci de l'appeler.

Je vois qu'Abdalmonem a tapé sa question. Je vais mettre sa question dans la liste plutôt que de lui passer la parole puisqu'il l'a tapée, et nous attendons toujours Patrick.

Je vous rappelle que les diapositives seront disponibles sur le wiki de l'ICANN. Et bien sûr, tout ceci sera également disponible sur ICANN Learn.

YEŞIM NAZLAR : Désolée, j'attends toujours que Patrick m'envoie son numéro pour que je puisse le rappeler. Désolée, nous n'avons pas de réponse de lui pour l'instant.

JOANNA KULESZA : S'il y a des commentaires des participants, n'hésitez pas à en faire part également.

YEŞIM NAZLAR : Je vais essayer de voir si je trouve son numéro dans la liste. Ah, voilà, voici son numéro. Maintenant, on devrait pouvoir le joindre par téléphone.

JOANNA KULESZA : Merci beaucoup Yeşim.

Merci Abdalmonem pour ce feedback très positif. Je dois dire que nous sommes très heureux de voir le nombre de personnes qui ont participé à ce webinaire et j'espère que nous pourrons continuer sur cette lancée et organiser davantage de webinaires suite à Marrakech puisque cela est apprécié.

Si vous souhaitez envoyer un commentaire, n'hésitez pas. Joan, vous souhaitiez peut-être faire un commentaire ?

PATRICK JONES : Me voici, je suis de retour. Même dans notre monde, nous avons des problèmes d'internet. C'est très frustrant, n'est-ce pas ? Merci beaucoup pour votre patience.

JOANNA KULESZA : Il y avait Joan au micro qui voulait poser une question, donc je vous suggère de lui passer la parole. Et ensuite, j'ai d'autres questions qui sont arrivées dans le chat. Peut-être que les interprètes pourront rester un peu plus longtemps avec nous pour répondre à toutes les questions.

PATRICK JONES : C'est bon, je vais donc répondre aux questions par téléphone. J'espère que la connexion sera bonne.

JOANNA KULESZA : Très bien, donc je vais passer la parole à Joan et je vais demander si les interprètes peuvent rester avec nous un peu plus longtemps. Joan, c'est à vous.

JOAN KATAMBI : Bonjour. Je suis de l'Ouganda. Est-ce que vous m'entendez bien ?

PATRICK JONES : Oui, ça va.

JOAN KATAMBI : Ma question, Patrick, est la suivante. Merci beaucoup pour la présentation.

Il y a les politiques de l'ICANN qui sont disponibles pour le public mais est-ce que l'ICANN a une stratégie en matière de cybersécurité qui est disponible et qui peut être accessible au public ? Voilà mes deux questions, la politique et l'accessibilité de cette politique.

PATRICK JONES : Partons à la deuxième question. Il ne s'agit pas d'une stratégie sur la cybersécurité mais c'est en fait un plan général qui comporte des éléments de sécurité. Nous avons récemment publié notre plan stratégique pour 2021-2025 et deux des cinq objectifs stratégiques sont relatifs aux DNS et à la sécurité des identificateurs uniques.

Donc si vous regardez un petit peu ce qui s'est passé avant, nous avions un cadre sur la sécurité et la sécurité et la résilience. C'est un document qui est publié sur le site de l'ICANN même si ce travail est en cours de mise à jour. Il y a une équipe de révision qui s'occupe en fait de toutes les questions relatives à la sécurité, la stabilité et la résilience. Donc voilà les documents que vous pouvez maintenant consulter. Nous n'avons pas un plan sur la sécurité mais le plan général stratégique de l'ICANN comporte des éléments de sécurité.

La première question, c'était quoi ? Est-ce que vous pourriez la répéter s'il vous plaît ?

JOAN KATAMBI : Est-ce que l'ICANN a une politique de cybersécurité qui est en place ? Par exemple en Ouganda, nous avons une politique sur la cybersécurité mais la stratégie est en cours d'approbation.

PATRICK JONES : Pour les réseaux sur lesquels nous fonctionnons, nous avons des politiques internes sur l'utilisation de nos systèmes de réseau, mais ce n'est pas un document qui a été publié. Nous avons une déclaration de mise en œuvre des extensions de sécurité pour les noms de domaine mais ce n'est pas vraiment votre question. Je ne crois pas que nous ayons des politiques de cybersécurité pour l'organisation sous forme de document public, mais nous avons des pratiques internes en fait.

JOANNA KULESZA : Merci Patrick.

J'ai encore trois autres questions. Est-ce que je peux vous les lire, Patrick ? Nous avons aussi demandé aux interprètes qui ont gentiment accepté de rester avec nous jusqu'à 15:10, donc nous avons encore dix minutes.

Je vais vous lire les questions et ensuite, je vais rouvrir à la liste des intervenants s'il y a d'autres demandes d'intervention.

Première question de [inintelligible] qui veut savoir : « Comment est-ce que les questions éthiques du DNS devraient être abordées ? » ; c'est la première question.

Deuxième question de Ibtissam Kaifouf qui veut savoir : « Quelles sont les questions de sécurité du DNS qui se posent par rapport aux technologies 5G et 6G ? »

Et dernière question d'Abdalmonem Galila qui voudrait savoir : « Dans le contexte des nouveaux protocoles du DNS comme DoH et DoT, est-ce

que l'ICANN devrait en particulier pousser davantage vers le DNSSEC et vers les protocoles liés au DNS ? »

J'espère que ces questions sont claires, sinon n'hésitez pas à demander plus de précision. Je vous cède la parole, Patrick. Si vous avez de précisions, n'hésitez pas.

PATRICK JONES : Alors par rapport aux questions éthiques du DNS, là, on doit être très prudents parce qu'en fait, l'ICANN n'est pas impliquée dans les questions liées au contenu sur le DNS. Notre travail se concentre uniquement sur les questions politiques et techniques par rapport au fonctionnement du système. Donc s'il y a des questions qui relèvent de la manière dont les identificateurs sont utilisés par rapport au contenu, ces questions échappent à la mission de l'ICANN. On peut offrir une plateforme pour les parties prenantes intéressées par cette question, on a une unité constitutive qui participe à ce travail, l'unité constitutive de la propriété intellectuelle qui effectue un travail au sein de l'ICANN, mais les questions liées au contenu, je pense que c'est la question qui est posée ici lorsque vous parlez des questions éthiques, cela ne relève pas des fonctions de l'ICANN. J'espère avoir répondu à votre question.

Pour la question suivante, question de sécurité liée aux technologies 5G et 6G, en fait, cette question porte sur les technologies émergentes. Et on a eu un forum DNS à Dubaï en février et l'un des co-organisateurs de l'évènement était un opérateur qui a parlé justement des questions liées à la technologie 5G. On parle dans nos réunions de l'évolution des technologies de l'internet donc cela pourrait être une question posées à Marrakech puis à Montréal, mais je pense qu'on va parler de plus en

plus de cela, notamment avec l'un de nos partenaires, GSMA, qui est une organisation qui chapeaute les opérateurs et qui travaille sur la mise en œuvre du 5G ; ils vont venir à nos réunions et on va certainement en parler beaucoup plus.

Et par rapport à la question d'Abdalmonem par rapport à DoH et DoT, effectivement, ce sont des questions qui intéressent beaucoup les gouvernements, les fournisseurs de service internet et bien d'autres et qui sont liées aux questions liées à l'évolution du DNS. Et l'ICANN a un intérêt pour faciliter les discussions autour de ce protocole au Maroc. Aux réunions suivantes en tout cas, sachez qu'on va certainement parler une fois et encore de cette question.

JOANNA KULESZA : Merci beaucoup Patrick, très intéressant. Je vois qu'Abdalmonem a répondu « OK » sur le chat, donc il est satisfait de votre réponse.

On a encore quatre minutes. Je ne sais pas s'il y a d'autres questions ou commentaires. N'hésitez pas à lever la main. Je ne vois pas d'autres questions sur le chat. Je ne sais pas si vous souhaitez soulever un autre point, poser une autre question ? Vous pouvez le faire maintenant. Il semblerait que tous les participants sont satisfaits de toutes les informations fournies et partagées. Je vais donc clore ce webinaire.

Merci énormément Patrick du temps que vous nous avez consacré et des difficultés techniques que vous avez surmontées pour nous rejoindre. Merci à tous d'avoir participé à ce webinaire et d'avoir participé aux cinq webinaires obligatoires. Merci à notre personnel sans lequel nous n'aurions pas pu organiser ce webinaire. Et enfin mais tout

aussi important, merci énormément aux interprètes qui ont fait de ce webinaire un échange international et très intéressant. Voilà.

Sachez que les webinaires sont disponibles sur l'espace wiki. La présentation figure d'ores et déjà sur la page wiki et ce sont des documents qui sont disponibles en ligne.

Si vous avez d'autres questions, n'hésitez pas à me joindre moi ou Alfredo, on pourra vous aider.

On attend avec impatience de vous retrouver à ATLAS, à At-Large ou autre. Merci à tous et bonne journée.

YEŞIM NAZLAR : Merci à tous de nous avoir rejoints pour ce webinaire d'aujourd'hui. Ce webinaire est maintenant terminé. Très bonne journée à tous. Au revoir !

[FIN DE LA TRANSCRIPTION]