YESIM NAZLAR : Cette réunion est maintenant enregistrée.

Bonjour, bonsoir à tous nos participants, bienvenue à ce deuxième webinaire At-Large sur l'utilisation malveillante du DNS. Nous sommes lundi 4 mai 2020 à 15 h UTC.

Nous n'allons pas faire l'appel aujourd'hui pour ne pas perdre de temps, mais nous allons prendre l'assiduité et tous les participants qui sont au téléphone, nous allons leur demander de bien se mettre sur mode silencieux pour qu'il n'y ait pas de bruit. Et veuillez indiquer votre nom lorsque vous prenez la parole pour que nous puissions vous interpréter et prendre en compte vos propos.

Donc, restez en mode silencieux pendant toute la présentation. Et donc avant la séance de question/réponse, vous pouvez utiliser le chat, la fonction chat sur zoom pour communiquer avec les autres participants.

Nous avons l'interprétation en langue espagnole et française. Vous avez un lien également sur la transcription en temps réel. Merci à toutes et à tous de vous être joint à nous.

Je donne maintenant la parole à Jonathan Zuck, co-président de l'ALAC.

JOANNA KULESZA : Bienvenue à toutes et à tous à ce deuxième webinaire du groupe de travail. Nous allons vous donner des informations sur l'utilisation malveillante du DNS et nous aurons plus tard une séance de

question/réponse. Nous parlerons également de l'importance de l'utilisation malveillante du DNS durant la pandémie de Covid 19.

Donc nous vous remercions de votre participation, nous remercions également les personnes ayant organisé ce webinaire. Merci à Jonathan et à Drew Bagley qui va nous parler un petit peu du rôle de la pandémie durant l'utilisation malveillante du DNS.

Nos intervenants fournissent des informations et nous pourrons leur poser des questions en fin de séance. Sans plus attendre, j'aimerais donner la parole à Jonathan Zuck et à notre invité pour parler de cette utilisation malveillante du DNS durant ce webinaire.

JONATHAN ZUCK : Merci beaucoup, Joanna, merci à toutes et à tous de vous joindre à nous.

Donc j'ai préparé une courte vidéo. Je vais vous présenter la vidéo et ensuite nous pourrons parler un petit peu plus.

Donc bonjour, bon après-midi et bonne soirée, et pour les moins fortunés bonne nuit. Aujourd'hui nous allons parler de l'utilisation malveillante du DNS qui est encore pire durant cette période de pandémie Covid 19.

On entend beaucoup parler de cybercriminalité, mais qu'est-ce que l'utilisation malveillante du DNS ?

Vous connaissez bien ce qu'est maintenant le DNS, c'est un système sophistiqué de questions et de réponses qui vous permet de vous rendre là où vous voulez sur le WEB, c'est un peu comme une chasse au

trésor, vous demander à une personne le nom de la personne qui connait le numéro de la personne que vous souhaitez joindre.

Bien sûr, comme on dit dans les films, toutes ces questions peuvent vous amener à être remarqué par les mauvaises personnes. Parlez-en à Dorothée qui cherchait le magicien d'Oz.

Autrement dit, l'utilisation malveillante du DNS est une attaque ou une utilisation du DNS à des fins délictuelles. Certaines personnes vont analyser cette définition plus en détail en appelant cela les attaques contre le DNS, l'utilisation malveillante du DNS et les attaques en utilisant le DNS. Mais, dans ce cas particulier, nous appellerons cela l'utilisation malveillante du DNS.

Et c'est le moment de vous poser une question. Vous n'aurez pas le temps de vous endormir.

Première question, qu'est-ce que le DNS ? Est-ce que c'est la société de la nature du Delaware, la Division de la sécurité nucléaire ou le système du nom de domaine ?

Si vous avez choisi le système de nom de domaine, vous avez tout à fait raison. La société de la nature du Delaware, ça fait également partie du DNS, mais pas de la même manière.

Donc une des attaques les plus connues contre le DNS est le déni de service distribué ou DDOS. Ici un délinquant utilise un réseau d'ordinateurs zombie pour envoyer une telle quantité de requêtes que le serveur est surchargé.

Parfois un élément s'interpose entre vous et les serveurs auxquels vous demandez des informations. Cela est possible à travers une attaque de l'homme du milieu ou un empoisonnement du cache du DNS, autrement dit vos requêtes sont interceptées et vous recevez un numéro qui ne correspond pas à celui du site que vous voulez visiter.

Ces redirections du côté serveur peuvent être utilisées pour quelque chose appelé dévoiement, également appelé hameçonnage sans leurre. Ici vous êtes simplement redirigé vers un site qui ressemble à celui que vous vouliez atteindre, mais qui est configuré pour capturer vos identifiants de connexion. Vous pensez que vous vous connectez à votre banque, mais en réalité vous remplissez simplement un formulaire pour que les pirates puissent accéder à votre compte sur le site web de la vraie banque.

Un des abus les plus courants effectués à travers le DNS est l'hameçonnage. Une manière beaucoup moins complexe de vous amener sur le mauvais serveur c'est de vous demander simplement d'y aller. Dans ce cas vous recevez un email suggérant qu'il y a un problème concernant votre compte en banque et que vous devez vous connecter pour le régler. Cependant, quand vous cliquez sur le lien vous êtes redirigé vers un site de dévoiement. Ce procédé est appelé hameçonnage parce que vous êtes attiré vers un site frauduleux.

Voici un exemple de ce qu'un tel email pourrait vous dire. Vous pouvez voir qu'il y a des éléments clef dans cet email, vous voyez qu'il s'agit d'une situation d'urgence, exigeant d'agir sans trop réfléchir, et d'un appel à vous connecter à votre compte.

Bien sûr les emails ne sont pas le seul moyen utilisé pour vous amener à accéder à des sites frauduleux. Parfois il s'agit de pièces jointes contenant directement des logiciels malveillants.

Un point particulièrement préoccupant pour At-Large est celui des noms de domaine internationalisés ou ITS, c'est-à-dire les noms de domaine utilisant des caractères non latins. Ces domaines relativement nouveaux sont essentiels pour attirer les prochains 4 milliards utilisateurs d'internet. 70 % du monde utilise des alphabets non latins et en 2012 nous avons pu finalement enregistrer des noms de domaine dans des langues telles que le Russe, l'Arabe et le Chinois. Naturellement chaque nouvelle innovation entraine des innovations correspondantes de la part des délinquants, tel est le cas des IDN.

Il s'avère qu'un bon nombre de lettres des alphabets non latins ressemblent beaucoup à des lettres de l'alphabet latin. Qui savait qu'il y avait tant de façon d'écrire banque of America ? Lorsque quelqu'un voit l'une de ces orthographes, tout en lisant rapidement un email, qu'est-ce qui l'empêcherait de cliquer dessus, en plus de collecter vos informations d'identification.

Ha c'est le moment une nouvelle fois pour une question, un nouveau quizz. Qu'est-ce qu'une attaque de déni de service ? Quand une serveuse est fâchée contre vous, trop de requêtes d'un serveur web ou venir au magasin sans chaussures ? Et vous avez raison, c'est B, trop de requêtes pour un serveur web. Voilà ce qu'est une attaque par déni de service. Mais parfois, vous savez, ce sont les chaussures qui font les attaques.

En plus de collecter vos informations d'identification, ces emails et sites web frauduleux ont pour objectif principal d'implanter des logiciels dans votre ordinateur. Ces logiciels sont généralement appelés logiciels malveillants, mais il en existe de nombreuses variétés. Vous avez déjà entendu parler de ce type de programme et bon nombre d'entre vous, vos amis ou votre famille, en ont surement été victimes.

Bien que nous n'ayons pas le temps d'examiner en détail chacun d'entre eux aujourd'hui, il suffit de dire qu'il s'agit de logiciels espions ou de rançongiciel, vous n'en voulez pas dans votre ordinateur. Malheureusement les infections de logiciels malveillants sont en augmentation au cours des dernières années : plus de 700 % ! À titre d'exemple, les attaques de rançongiciels ont augmenté de 350 % en 2018 seulement.

En toute équité, en particulier après la révision de la concurrence, le choix et la confiance des consommateurs de la série de TLD en 2012, le département en charge de la conformité contractuelle de l'ICANN fait de son mieux. Il a commencé à publier des données beaucoup plus précises sur les plaintes et à rendre son processus de révision un peu moins aléatoire. Mais cela ne suffit toujours pas.

Vous avez peut-être entendu parler de quelque chose appelé DDAR, ou système de signalement des cas d'utilisation malveillante des noms de domaine mis en place il y a quelques années par ICANN. Les rapports mensuels fournissent juste assez de données pour savoir qu'il y a un problème, mais n'en fournissent pas assez pour en faire quelque chose pour éviter un domaine ou un bureau d'enregistrement qui ne semble pas honnête. En utilisant DDAR, nous pouvons déterminer que le

pourcentage de cas d'utilisation malveillante détecté a diminué de moins de 1 % depuis sa création il y a deux ans. Nous pouvons donc convenir que l'abus du DNS est un problème majeur pour les utilisateurs individuels.

Et bien, At-Large peut adopter une approche à deux volets pour lutter contre l'utilisation malveillante du DNS tout en réalisant un travail de sensibilisation et en contribuant à l'élaboration de politiques de l'ICANN. Du matériel éducatif sera donc adopté pour les utilisateurs finaux afin qu'ils puissent mieux se protéger. At-Large s'organise suivant une structure unique qui lui permet de diffuser des informations aux organisations régionales At-Large, aux RALO, qui à leur tour peuvent distribuer ces documents aux structures At-Large qui les composent, à leur tour formées de membres individuels auxquels ils peuvent distribuer le matériel. At-Large développe ce réseau depuis des années, et quoi de mieux que de protéger les utilisateurs contre les criminels sur internet. Il existe un certain nombre de messages que nous pouvons transmettre pour aider les gens à éviter les pièges qui leur sont tendus chaque jour.

L'ironie persistante est que les criminels obtiennent la plupart des informations dont ils ont besoin auprès des utilisateurs, non pas en étant des ingénieurs informatiques intelligents comme dans les films, mais en étant des ingénieurs socio-intelligents. En bref, s'ils veulent notre mot de passe, ils le demandent tout simplement. C'était vraiment internet, et ça l'est encore aujourd'hui. At-Large doit éduquer les utilisateurs à être à l'affut de nouvelles qui sont trop belles ou bonnes pour être vraies. Il existe des moyens de le faire.

Nous aimons nous moquer des emails d'hameçonnage, en raison des fautes de grammaire qu'ils contiennent. Ce que nous ne réalisons pas c'est que ces fautes sont intentionnelles, écrire de cette façon déclenche simultanément une suppression de la part de ceux qui reconnaissent l'arnaque et de l'attention chez ceux qui sont moins sophistiqués. At-Large veut certainement aider les utilisateurs finaux à discerner l'authenticité d'un email inattendu. Cela va sans dire, mais At-Large le dira quand même, les utilisateurs individuels devraient avoir un logiciel de protection antivirus sur leur PC et sur leurs appareils portables.

Mais le fait est qu'aux États-Unis, même aux États-Unis, où on s'attendrait à une sophistication considérable de la part des utilisateurs, près de 50 % des ordinateurs ne sont pas protégés contre les virus. At-Large doit encourager les utilisateurs finaux à demander à leurs employeurs s'ils ont des serveurs compatibles avec le DNSSEC pour prévenir des évènements tels que les attaques de l'homme du milieu.

Par ailleurs, At-Large doit se faire entendre dans les couloirs, les réunions et les conférences téléphoniques qui intègrent le processus d'élaboration de politique de l'ICANN. At-Large se souciera de participer à l'élaboration de politique de l'ICANN à chaque étape du processus. Que ce soit une conversation dans un couloir ou à travers la participation à un groupe de travail ou à une équipe de révision. Nous nous impliquerons activement à la plaidoirie pour les réformes, à la fois au sein de l'ICANN et auprès des entreprises qui servent les utilisateurs finaux tels que les bureaux d'enregistrement et les opérateurs de registre.

Autrement dit, si quelqu'un nous interroge sur la météo, on tend la main, on lève les yeux vers le ciel, et on dit : la température ressentie suggère une utilisation malveillante du DNS.

Heureusement, nous ne sommes pas seuls. La majorité de la communauté de l'ICANN est préoccupée par les abus du DNS et hésite à autoriser une nouvelle série de TLD sans qu'il y ait une réforme exhaustive. Une minorité ne peut absolument pas être en mesure de lancer l'ICANN vers une nouvelle série sans la véritable adhésion du reste de la communauté. At-Large s'est associée et continuera de s'associer avec d'autres groupes au sein de la communauté de l'ICANN pour sonner le signal d'alarme concernant l'utilisation malveillante du DNS et promouvoir activement une réforme.

Notre première tâche est de maintenir notre proposition : aucune nouvelle série ne devrait pouvoir être lancée tant que l'utilisation malveillante du DNS n'a pas été atténuée de manière significative. Le département en charge de la conformité a besoin d'une vision holistique de l'utilisation malveillante du DNS. Il ne peut pas simplement réagir aux plaintes, mais doit utiliser son pouvoir de supervision pour reconnaitre les pourcentages d'utilisation malveillante et prendre les mesures contre les TLD, les opérateurs de registre et bureaux d'enregistrement qui font partie du problème. Délimiter les enregistrements volumineux, car il existe une forte corrélation avec l'utilisation malveillante du DNS. Bien sûr, il existe des utilisations légitimes pour les enregistrements groupés et ses usages ne pourront qu'augmenter avec l'internet des objets, mais At-Large continuera de plaider pour une vérification accrue d'une telle activité.

L'équipe de révision de la conformité et par conséquent l'équipe de révision de la sécurité et de la stabilité ont toutes deux suggéré que l'ICANN conçoive des incitations pour adopter les meilleures pratiques. Il est certain que davantage de recherches peuvent être effectuées et ont été recommandées par la CCTRT, la SSRT, l'ALAC et maintenant VeriSign. Le budget a maintenant été débloqué de 20 millions de dollars de plus l'investissement dans la sécurité et la stabilité du DNS.

Il y a certainement des opérateurs de registre et des bureaux d'enregistrement qui investissent beaucoup de temps et d'argent dans la lutte contre l'utilisation malveillante. De fait, 48 entreprises ont signé un engagement envers les meilleures pratiques. Et c'est très bien, mais nous avons encore besoin de réformes pour mieux cibler les mauvais acteurs. Et franchement, même les bons acteurs pourraient mieux faire. C'est pourquoi At-Large ne doit pas baisser les bras non plus. C'est comme cette vielle BD de [Guilbert] dans laquelle on nous rappelle qu'une fois que tout le monde a adopté les soi-disant les meilleures pratiques, ces pratiques deviennent la nouvelle norme et ne sont plus les meilleurs. Les délinquants ne sont pas satisfaits de la situation actuelle et nous ne pouvons pas non plus nous permettre de l'être. Même les gentils peuvent mieux faire.

Tout cela pour dire qu'il s'agit d'une situation de crise ou personne n'est à l'abri. Des recherches incroyables sont en cours dans l'apprentissage automatique pour mieux détecter les abus en temps réel, et prédire si un enregistrement est destiné à un usage illégal. Les premiers tests de cette technologie par .EU montrent une précision de près de 80 % dans ces prévisions. Nous devons nous assurer que ces recherches se

poursuivent et que des systèmes soient mis en place pour nous protéger de la prochaine génération d'attaque.

Dernière question du quizz. Quels sont les outils pour lutter contre l'utilisation malveillante du DNS ? Éducation : A, B : DNSSEC ou C : Chiffrement ? Si vous avez choisi toutes les réponses, vous avez raison. SI ce n'est pas le cas, veuillez rester après ce cours.

Tout cela pour dire qu'il s'agit d'une situation de crise où personne n'est à l'abri. Des recherches incroyables sont en cours dans l'apprentissage automatique pour mieux détecter des abus en temps réel et prédire qu'un enregistrement est destiné à un usage illégal.

En fin de compte, il n'y a qu'une seule unité constitutive, celle des utilisateurs finaux. C'est pour protéger les intérêts de ces utilisateurs finaux qu'At-Large a été créé.

Merci à tous.

Bien, si vous avez des questions avant de passer à la présentation de Drew, n'hésitez pas à me les poser maintenant, je suis à votre disposition. Je ne vois aucune question, alors je m'adresse au personnel, est-ce que vous avez identifié des questions sur le chat que je n'aurais pas vu peut-être ? Oui, il y a une question me dit-on. Oui, allez-y.

[YESIM] : Jonathan, je voulais vous dire que je ne vois aucune question sur le format que nous avions préconisé pour que les participants puissent poser leurs questions…

Ha si, nous venons de recevoir une question de Raymond Mamattah.

JONATHAN ZUCK : Oui, je vois la question. Alors, la question, c'est par rapport au dévoiement. Est-ce que c'est un terme technique ou c'est une invention de ma part ?

En fait c'est un terme général, vous devriez trouver des références facilement sur le web. Et l'une des choses que l'on prévoit de faire à l'At-Large c'est de développer la page Wikipédia sur l'utilisation malveillante du DNS, parce que pour l'instant il n'y en a pas sur cette utilisation malveillante. Donc nous voulons développer et élaborer cette page pour que les gens puissent voir toutes les informations pertinentes par rapport à la cybercriminalité et à l'utilisation malveillante du DNS. Donc l'utilisation malveillante c'est en fait une sous-partie de la cybercriminalité.

Bien, alors Drew je vais maintenant vous céder la parole. C'est à vous.

DREW BAGLEY : Merci Jonathan. Est-ce que vous voulez que je partage mon écran pour faire défiler la présentation.

YESIM NAZLAR : Oui, oui bien sûr Drew.

DREW BAGLEY : Permettez-moi quelques instants.

NON IDENTIFIÉ : Une question de Glenn sur le chat.

JONATHAN ZUCK : Oui, je vois la question de Glenn sur le chat, mais je ne suis pas bien sûr de la comprendre. Est-ce que vous avez vu une résurgence du terme hameçonnage pendant la crise du Covid 19 ? C'est ça la question ?

Oui, bien sûr, on a vu beaucoup d'augmentation de l'utilisation de ce terme hameçonnage, est-ce que c'est ça la question ?

Écoutez, si je n'y ai pas répondu, attendons la fin de la présentation de Drew, et j'y répondrai.

DREW BAGLEY : Merci. Je sais que beaucoup d'entre vous me connaissent déjà. Mais pour ceux qui ne me connaissent pas, je m'appelle Drew Bagley, je travaille pour la Secure Domain Fondation qui travaille pour lutter contre l'utilisation malveillante du DNS, et président d'un groupe de travail et entreprise de cybersécurité.

Donc, ma présentation aujourd'hui va vous permettre de mieux comprendre ce que nous avons vu en termes de menaces à l'utilisation malveillante du DNS en cette période de crise du Covid 19 et élaborer et développer un peu plus ce que Jonathan nous a présenté dans la vidéo. Donc moyens pour identifier et lutter contre l'utilisation malveillante du DNS.

Donc certaines des tendances qui ont été observées au cours des deux derniers mois en cette période de pandémie du Covid 19 c'est que les mauvais acteurs sont en train de tirer partie de tout type de situation,

en raison de cette pandémie. Et il est assez intéressant de voir qu'il y a un certain nombre de tendances qui émergent qui fait que les vulnérabilités de gens sont un peu différentes d'un point de vue social et technique, mais aussi du côté de l'ingénierie.

En effet, en fonction de l'endroit où vous êtes, du secteur dans lequel vous travaillez, si vous travaillez depuis chez vous ou pas, il y a toute une série de situations de travail actuellement, parce que dans certaines organisations on a pu mettre en place des dispositifs pour que les gens télétravaillent, et dans d'autres, il faut que les gens utilisent leur propre ordinateur pour travailler depuis chez eux. Donc, ça fait que vous avez moins de contrôle sur la cybersécurité et les données.

Et à cela s'ajoute le sentiment chez nous tous de vouloir trouver plus d'informations sur le Covid 19, et donc un environnement où il y a des attaques de hameçonnage ou des attaques où on essaie de profiter des gens qui cherchent des informations sur le Covid 19 et des gens qui utilisent des dispositifs personnels sans aucun type de sécurité, aucun pare-feu ou aucun type de sécurité sur leur dispositif personnel.

Donc il y a des noms de domaine qui ont enregistré le terme Covid 19 ou des organisations avec le terme WHO, l'acronyme de l'OMS en anglais et qui se présentent comme des sites légitimes. Donc il y a eu beaucoup de campagnes et je vais vous donner quelques exemples qui ont eu lieu de par le monde.

Vous voyez ici une organisation australienne qui met en garde les gens contre une campagne d'hameçonnage pour recherche d'information autour de la crise de COvid 19. Donc vous voyez ici, COVID19-INFO.ONLINE et là vous allez sur ce site web et vous recevez des

messages texto pour essayer que les gens aillent sur le lien, cliquer sur le lien sur leur téléphone portable. Et ce lien peut être utilisé pour déployer des logiciels malveillants.

Il y a eu d'autres campagnes aussi qui sont très semblables, au Royaume-Uni par exemple, où il y avait ce nom de domaine UK-COVID19-RELEAVE.COM et ce même domaine essayait de faire en sorte que les gens cliquent sur ce nom de domaine pour aller sur un site web où les victimes allaient rentrer leurs données personnelles, comme leur numéro de passeport ou d'autres types d'informations à caractère personnel, et les délinquants allaient s'en approprier pour usurper leur identité, commettre des délits ou autre.

Et dans ces deux cas, vous le voyez, je vais revenir en arrière, nous avons ici les informations qui vous montrent que les noms de domaine ont été enregistrés très récemment, donc très souvent, quand vous vérifiez l'authenticité d'un nom de domaine vous observez un certain nombre de variables, dont l'une quelle est la date d'enregistrement du nom de domaine, et là on voit le début de la pandémie, donc c'est récent. Et donc ça, en soi, c'est une information suspicieuse. Et ensuite vous avez toutes les informations concernant l'enregistrement et là, la société d'anonymisation est basée au Panama, donc là encore c'est suspicieux. Et il faut comprendre si un nom de domaine est légitime ou pas.

Et bien sûr, comme Jonathan l'a dit, il faut voir un certain nombre de choses. D'abord, assurer un suivi du nom de domaine en consultant WHOIS, et il y a des détails qui sont cachés qui peuvent vous dire si ce nom de domaine est effectivement suspicieux ou pas. Et il faut se poser

la question si vous pouvez faire confiance à ce nom de domaine. Et vous pouvez le voir ici dans ces deux cas.

Donc je n'ai pas de musique, comme Jonathan avait tout à l'heure, mais je vais vous poser quand même quelques petites questions.

Première question : est-ce qu'il est facile de savoir si un email est légitime ? Vrai ou Faux. Donc je vous donne 5 secondes de plus pour trouver la réponse. Très bien. Et la réponse c'est Faux. Ce n'est pas toujours facile de savoir si un email est légitime ou pas. Parce que l'ingénierie sociale, c'est un art, véritablement, et il y a des personnes très fortes dans cet art. Ça peut être très spécifique, très ciblé, quelqu'un d'associé à une organisation peut s'attendre à ce type d'email, à le recevoir. Et, très souvent, ils font donc du dévoiement avec des informations d'enregistrement et ainsi de suite, c'est parfois très bien réalisé, et l'adresse semble être une adresse tout à fait valide. Donc je vais vous donner des exemples de cela, et vous allez pouvoir voir que la plupart d'entre vous ont dit faux, c'est correct. Il y a des personnes qui vous disent : non, on peut trouver facilement que c'est un email frauduleux, je vais vous donner quelques exemples, vous allez pouvoir juger.

Regardez là, vous pouvez voir que ça semble venir d'un nom de domaine légitime, avec une adresse email tout à fait légitime associée avec l'OMS, l'Organisation mondiale de la Santé, et il y a des campagnes qui existent, qui sont tout à fait légitimes. Donc là, vous voyez avec [.INP], [inaudible CITIES@WHO pour OMS], vous voyez cela à l'écran, et en fait l'adresse de retour ne va pas être la bonne, et ça, ça va être du dévoiement.

Donc pour éviter cela, les organisations doivent vraiment assurer la sécurité de leurs serveurs email et donc déployer diverses technologies. Mais, néanmoins, c'était très courant cela, où les emails semblent tout à fait légitimes.

Peut-être que ce serait difficile d'avoir l'en-tête de l'OMS, mais le reste du courriel de l'OMS peut paraitre tout à fait légitime. Donc il y a tout ce travail qui est fait à l'imitation des différents graphiques. Donc vous voyez ces exemples, et il est difficile de dire la différence.

Donc vous avez différents blogs que vous pouvez voir également en bas de l'écran. Un blog de [Crowdstrike]

Donc pour rester en toute sécurité, comme Jonathan l'a dit tout à l'heure, il est extrêmement important lorsque que vous recevez un SMS ou un courriel ou tout autre type de communication qui a un lien ou qui vous demande d'agir, de faire quelque chose, envoyer de l'argent, il est extrêmement important de scruter de très près tout cela avant de vous connecter.

Alors, inspectez l'email, inspectez l'en-tête, ça ne suffit pas néanmoins. Essayez d'utiliser le WHOIS pour voir si ce nom de domaine est enregistré à bon escient et peut-être qu'il y a également des systèmes qui permettent de se cacher, même si le WHOIS semble bon. Mais considérez l'entièreté de la communication. Et également, réfléchissez à qui vous contacte. Peut-être que vous pouvez essayer de les appeler, peut-être que dans l'exemple de l'OMS il y a le site web de l'OMS, peut-être que sur le site web de l'OMS vous allez pouvoir trouver des informations qui vont vous permettre de limiter cette usurpation d'identité.

Vous savez, en Australie, il y a eu des exemples comme cela d'utilisation malveillante. Donc dans ces cas, le nom de domaine n'avait pas encore été retiré et il y a des personnes qui ont perdu de l'argent, qui ont envoyé de l'argent à ces escrocs.

Et assurez-vous également que vous protégez bien vos appareils. C'est extrêmement important d'avoir des solutions de sécurité, antivirus et ainsi de suite. Il faut mettre à jour vos logiciels. Il y a des logiciels qui vous permettent de mieux vous protéger, de protéger vos ordinateurs, pour que vos ordinateurs ne soient pas redirigés vers ces escrocs. Donc ça peut être au niveau de votre employeur, au niveau de vos ordinateurs personnels.

Donc la formation cybersécurité est extrêmement importante et elle doit être fournie par votre employeur, votre organisation ou association.

De même, pour tester les URL, les adresses universelles, c'est d'utiliser des sites multi scanners, qui sont gratuits, comme hybrid-analysis.com que vous voyez à l'écran. Ça permet de faire des tests sur les différentes adresses. Ça peut être très utile. Donc, allez sur un site de cybersécurité avant donc de communiquer.

Deuxième question du petit questionnaire, qu'est-ce qu'un exemple d'anti-abus proactif ? Est-ce que c'est la recherche d'un nom de domaine après son utilisation pour du fishing ? Vous avez à l'écran les différents choix. Je vais vous donner 15 secondes de plus pour répondre.

Et bien la réponse finale s'il vous plait. Alors il semble que nous avons les résultats maintenant… Donc vous avez C et D. Si vous faites quelque chose une fois que ça a été utilisé, l'utilisation avant qu'il ne soit utilisé. Je vous ai montré cela, c'est très important, de découvrir avant d'agir et de communiquer. Et il peut y avoir tout un compte associé à cela. Donc ça, c'est un exemple d'utilisation malveillante. Mais il y a d'autres activités, comme nous l'a indiqué Jonathan, qui font partie de l'abus du DNS. Vous pouvez identifier donc, bien en avance, ces domaines frauduleux qui font de l'hameçonnage, une campagne d'hameçonnage, au niveau de l'enregistrement par exemple.

De même, s'il y a des comptes de titulaires de noms de domaine qui sont associés à des sites d'hameçonnage, du hightjacking, et bien tout cela, c'est quelque chose qui vous indique qu'on ne peut pas se fier à ces personnes. Il y a des noms de domaine qui sont constamment ajoutés pour l'utilisation malveillante.

Donc voilà les résultats. Non, pas mal, vous avez bien répondu je trouve.

Donc ce qui est intéressant, c'est qu'il y a beaucoup d'incitations pour les personnes qui pourraient être des victimes.

Il y a beaucoup d'organisations au niveau juridiques qui peuvent être utiles, et véritablement c'est vraiment une situation grave, et ça profite uniquement aux criminels. Donc les ccTLD et les personnes ayant des noms de domaine gTLD, doivent absolument, dans le cadre de leur contrat, ne pas permettre cette utilisation malveillante. Ils doivent se conformer contractuellement pour empêcher justement, et risquent des poursuites judiciaires. Parce qu'il y a la réputation également qui est très importante. Il faut être un bureau d'enregistrement réputé pour ne

pas avoir de problème, ne pas être bloqué, ne pas avoir des problèmes avec les forces de l'ordre et les autorités. Parce que dans un TLD il y a beaucoup d'abus, et bien on ne va pas leur faire confiance et on ne va pas s'enregistrer avec eux.

Donc il y a ces problèmes avec l'argent qui doit être renvoyé sur les cartes de crédit, il y a même des poursuites judiciaires possibles, donc tout le monde doit être extrêmement proactif et lutter contre cette utilisation malveillante.

Mais pourtant avec le Covid 19 nous voyons que de plus en plus de noms de domaine, très facilement, font de l'usurpation d'identité et ces sites réussissent à s'inscrire auprès de bureaux d'enregistrement, et existent, c'est une situation grave, malgré tous les problèmes qu'ils risquent d'avoir. Et bien il faut identifier absolument ces sites web et scruter tout ce que l'on fait sur l'internet pour ne pas être une victime.

Et bien nous allons passer à notre troisième question de notre petit questionnaire. Qui est affecté par un abus du DNS, une utilisation malveillante du DNS ? Alors, est-ce que c'est l'ICANN, les parties contractantes, les utilisateurs finaux qui cliquent sur les liens et uniquement eux, les consommateurs ou toutes les personnes ? Je vous donne 15 secondes de plus.

Très bien, je crois qu'on a reçu beaucoup de retour de votre part sur ces questions. Excellent, très bien, toutes les personnes sont affectées par l'utilisation malveillante du DNS, c'est la bonne réponse. Au niveau financier, pour les entreprises, pour tout le monde, tous les utilisateurs finaux sont impactés à un moment ou à un autre, les organismes, les associations qui ont en leur sein des utilisateurs finaux. Et bien tous

ceux-là représentent des personnes qui sont affectées par l'utilisation malveillante du DNS. On a vu des attaques nombreuses ces dernières années, de rançongiciels, avec [KAPCHA] qui a dû être mis en œuvre. Nous avons vu beaucoup d'exemples récemment, et tout le monde peut être affecté par la cybercriminalité. Par exemple, au niveau des enregistrements, il y a eu la possibilité de déployer des logiciels malveillants, et il y a eu des données qui ont été volées, donc tout le monde est impacté.

Bien, nous allons passer à la question suivante. Qui a la capacité de lutter ou de prévenir l'utilisation malveillante du DNS ? Alors, je ne sais pas si la question que je viens de vous poser est affichée à l'écran actuellement. Est-ce qu'on pourrait m'aider s'il vous plait à l'afficher à l'écran ?

NON IDENTIFIÉ : Je ne sais pas si vous trouvez le bon icone pour afficher la question.

DREW BAGLEY : La voici, elle est à l'écran.

Qui a la capacité d'empêcher les abus DNS ? Je vais vous laisser 15 petites secondes pour répondre à cette question.

Bien, alors, pour ceux qui ont répondu : nous le faisons tous, c'est-à-dire que nous avons tous, la Communauté ICANN et l'ICANN en tant qu'organisation ont un rôle à jouer important, les parties contractantes sont en première ligne bien entendu face à cette situation, sont très proactifs pour signaler un enregistrement abusif, pour s'assurer qu'une

campagne d'hameçonnage ou autre puisse être finalisée. Les utilisateurs finaux également qui peuvent se protéger et signaler ce genre d'abus. Également les experts en cybersécurité qui sont en première ligne pour signaler ce genre de chose, donc toute la communauté de cybersécurité analyse ce genre de choses et met en œuvre tous les moyens nécessaires pour lutter contre l'utilisation malveillante du DNS et protéger les utilisateurs finaux. Donc la réponse c'est : nous le faisons tous.

Pour conclure, je dirais que la gouvernance de l'internet est très importante pour lutter contre les utilisations malveillantes du DNS, c'est la raison pour laquelle, comme Jonathan l'a dit avant moi, la communauté At-Large joue un rôle clef, puisqu'elle représente les utilisateurs finaux, pour s'assurer qu'en fin de compte les utilisateurs finaux sont écoutés, entendus, pour expliquer, éduquer et promouvoir des solutions politiques qui peuvent réellement avoir un impact sur l'utilisation malveillante du DNS. Et que ce soit l'ALAC ou d'autres parties de la communauté ICANN, l'ICANN et la communauté peuvent créer des encouragements pour s'assurer qu'il y a un terrain d'entente entre tous. Et tout le monde devrait participer à cette lutte. Et la communauté peut entreprendre des mesures d'atténuation d'utilisation malveillante du DNS, être plus proactive pour l'utilisation malveillante du DNS, et trouver des moyens pour prévenir ce genre d'exemples très simples que je vous ai montrés aujourd'hui, pour que ce genre d'hameçonnage, usurpation d'identité, en temps de Covid 19, puisse ne pas avoir lieu. Donc que ce genre d'exemples n'aient pas lieu.

Et c'est donc là que cette unité constitutive et la communauté en général peut jouer un rôle fondamental pour lutter contre l'utilisation

malveillante du DNS. Et avec certains des aspects dont Jonathan a parlé le DDAR, le signalement des cas d'utilisation malveillante des noms de domaine, on voit qu'une approche fondée sur les données peut être utilisée, parce que cela nous montre de quelle manière l'utilisation malveillante du DNS est perpétrée, de quelle manière les registres sont utilisés pour enregistrer un certain nombre de noms de domaine et à quelle fin. C'est pourquoi il est important maintenant de prendre ces données et faire quelque chose au niveau de la gouvernance de l'internet par rapport à l'utilisation malveillante du DNS.

Bien, nous avons fini le questionnaire, mais j'ai encore quelques questions supplémentaires à vous poser.

La première : est-ce vous-même vous avez reçu des campagnes de hameçonnage liées au Covid 19, pas forcement celles que je vous ai montrées, mais d'autres, que ce soit par internet ou par mail. Je vous laisse cette question à l'écran encore 15 secondes supplémentaires.

NON IDENTIFIÉ : En fait il y a deux questions, donc il faudrait faire défiler pour qu'on voie les questions.

DREW BAGLEY : Deuxième question, c'est vrai, est-ce que vous avez reçu des informations supplémentaires concernant la cybersécurité de la part de votre employeur depuis que la pandémie du Covid 19 a commencé ? Je vous laisse encore 5 secondes pour y répondre.

NON IDENTIFIÉ : Bonjour. Allo ? Est-ce que je peux intervenir ?

NON IDENTIFIÉ : Il s'agit de quelque chose que vous avez partagé sur votre écran ?

DREW BAGLEY : Oui, il y a deux questions partagées à l'écran, et maintenant on va partager les réponses.

Donc, malheureusement pour ceux d'entre vous qui ont répondu oui, ils ont été ciblés par des campagnes d'hameçonnage pendant la crise du Covid 19. La moitié d'entre vous considère qu'ils n'ont pas été ciblés. Et, il semblerait que seuls 26 % d'entre vous ont reçu une formation supplémentaire en termes de cybersécurité.

Je vous l'ai dit au début de cette présentation, je pense que c'est particulièrement important maintenant parce que très souvent les dispositifs de télétravail sont différents. Vous pouvez avoir des dispositifs professionnels que vous a donnés votre employeur, ou bien vous travaillez sur vos dispositifs personnels et ça, ça fait une grande différence.

Et même si ça, ça n'a pas changé, peut-être que vous n'êtes pas au courant de ces dernières pratiques en temps de pandémie pour toucher les gens. Et ça, c'est très important pour que vous ayez ces informations, que votre employeur vous fournisse cette formation et ces informations nécessaires pour lutter contre l'utilisation malveillante du DNS.

Voilà, j'en ai fini avec ma présentation, mais je suis à votre disposition si vous avez des questions. Je vais regarder le chat.

JONATHAN ZUCK : Alors il y a eu plusieurs questions qui ont été posées. L'une d'entre elles est la suivante : on voit en général que les bureaux d'enregistrement ne sont pas réactifs aux demandes d'information. Avez-vous des exemples d'opérateurs de registre ou de bureaux d'enregistrement qui ont été utiles ou qui ont aidé à apporter une réponse.

DREW BAGLEY : Oui, j'aurai tendance à dire que ces deux situations se produisent sans arrêt. Donc les bureaux d'enregistrement et opérateurs de registre, ça dépend beaucoup du type de bureau d'enregistrement et d'opérateurs de registres. Et ça dépend aussi de la situation et du niveau d'attention reçu par le nom de domaine à un moment donné.

Ce que je sais c'est qu'il y a des situations où les parties en se montrent pas réactives. Donc je n'ai pas d'exemple spécifique à partager avec vous où les bureaux d'enregistrement ou opérateurs de registre auraient été réactifs, mais on voit que ça dépend donc des parties et que parfois elles sont très réactives. Donc c'est très bien de réagir, mais ce n'est pas la même chose que de trouver des moyens d'être proactif lorsqu'un enregistrement apparait et qu'il est utilisé pour porter atteinte aux individus.

Donc il est important que les gens insistent s'ils veulent porter plainte contre un opérateur de registre ou un bureau d'enregistrement pour utilisation malveillante du DNS. Donc la conformité c'est important si les

opérateurs de registre ou bureau d'enregistrement ne respectent pas leurs engagements contractuels.

Et il y a aussi les recommandations de l'équipe de révision CCT qui doivent être mises en œuvre pour s'assurer que ces deux parties soient réellement plus proactives.

JONATHAN ZUCK : Merci. Autre question sur le chat, de Samridh Kudesia. Je n'ai pas vraiment compris de quelle manière les informations dans le chapeau, l'intitulé sont différentes des autres informations.

DREW BAGLEY : En fait, ça peut se produire de plusieurs manières, et ça dépend de la manière dont les serveurs sont configurés. Parfois, dans le serveur sortant de mail il n'y a pas les mêmes paramètres de sécurité que par rapport aux mails rentrants. Donc une personne qui n'est pas affiliée à une organisation peut donner des détails du serveur de mail sortant d'une organisation sans avoir aucune des informations d'identification. Ça, ce serait une manière de procéder. Parfois, ils n'utilisent pas un serveur légitime, ils font croire que l'intitulé vient d'un nom de domaine qui est très proche de celui qui est légitime, donc c'est parfois une seule lettre qui change. Donc voilà comment, en général, ils utilisent les serveurs de mail sortant.

JONATHAN ZUCK : Oui, même chose par rapport aux homonymes IDN. Je vous ai donné l'exemple de Bank of America avec l'écriture qui ressemble, mais il y a un caractère qui change.

Ensuite une question de [inaudible]. On ne pense pas qu'il existe à 100 % infaillible, sachant que 70 % sont internes à l'organisation. Que peut faire l'ICANN ?

DREW BAGLEY : Je pense que cette question s'adresse plus à l'organisation ICANN, puisque c'est une atteinte à l'organisation ICANN. C'est une violation de l'utilisation du DNS par rapport à des organisations qui aimeraient apporter une réponse en cas de violation et, en fin de compte, vous analysez toute l'infrastructure, les adresses IP, le titulaire de nom de domaine, etc., pour s'assurer que cette infrastructure est effectivement examinée, qu'il n'y a pas de violation. Mais, par rapport à l'organisation ICANN, c'est à elle de répondre aux menaces, et donc il faudrait poser cette question à l'ICANN directement.

JONATHAN ZUCK : Alors, une question de Hadia Elminiawi. Il y a beaucoup de données d'enregistrement de nom de domaine qui ont un impact négatif sur l'utilisation malveillante du DNS.

DREW BAGLEY : Alors, du point de vue de la cybersécurité, je dirais que l'une des choses que fait la communauté cybersécurité, au-delà de l'analyse de corrélation, c'est de voir même si vous avez un certain nombre

d'informations, si vous avez une adresse mail commune qui est utilisée, vous pouvez faire une requête vis-à-vis de cette adresse mail, et peut-être que vous trouverez qu'il y a des noms de domaine qui sont déjà utilisés pour des comportements suspicieux et ensuite des noms de domaine qui sont enregistrés et qui n'ont pas été utilisés, mais vous avez une suspicion alors c'est probablement le même titulaire de nom de domaine.

Et maintenant, avec les changements de WHOIS, c'est une corrélation qu'il est très difficile de mettre en œuvre. Cela étant dit, l'utilisation des services d'anonymisation, parce que la protection de la confidentialité existe depuis des années, mais la différence c'est que les délinquants cybernétiques n'ont pas toujours utilisé les services d'anonymisation, et ça représente des fonds supplémentaires, donc ça c'est des informations qu'il est difficile de trouver.

JONATHAN ZUCK: Et bien merci Drew. Prochaine question. Est-ce qu'il y a des applications gratuites qui pourraient améliorer la sécurité contre les logiciels malveillants, et qui sont disponibles et que vous connaissez Drew ?

DREW BAGLEY : Oui, tout à fait. J'ai fait référence dans ma présentation à HYBRID-ANALYTIS.COM. C'est une plateforme qui a beaucoup de travail de cybersécurité réalisé sur le site. Et il y a des rapports publics, et vous pouvez savoir, avec ce site si vous pouvez faire confiance à cette adresse email, et toutes les utilisations malveillantes sont donc notées. Il y en a d'autres qui existent. Vous avez ça dans la présentation.

JONATHAN ZUCK: Merci beaucoup Drew. Est-ce que l'utilisation malveillante du DNS c'est de l'espionnage commercial également ?

DREW BAGLEY : Ça peut être utilisé pour beaucoup de chose cette utilisation malveillante du DNS. Il y a des États en effet qui mènent cela pour leurs propres intérêts. Vous avez de la cybercriminalité, vous avez des activistes qui l'utilisent aussi, des hackers qui font de la disruption, donc ça peut être utilisé pour tout, pour tous les types d'abus du nom de domaine, du DNS.

JONATHAN ZUCK: Très bien, merci beaucoup. Donc peut-être que c'est pour le personnel, cela, ce point. Une question de Vivek, quel est le temps de réponse lorsqu'il y a une plainte ? Lorsqu'il y a des plaintes, combien de plaintes sont reçues et à quelle vitesse répond-on à ces plaintes, et qu'est-ce qui est disponible de public à ce sujet ?

DREW BAGLEY : Oui, ça je ne peux pas répondre à cela, c'est à l'organisation ICANN de répondre.

JONATHAN ZUCK Nous essaierons d'apporter une réponse à ce sujet par l'intermédiaire du groupe de travail et sur la page Wiki, à la suite de ce webinaire. Je crois que c'est toutes les questions que nous avons reçues.

Merci beaucoup Drew. Je vais redonner la parole à Joanna.

DREW BAGLEY : Merci Jonathan.

JOANNA KULESZA : Merci beaucoup, Drew et Jonathan, nous apprécions beaucoup le fait que vous avez pu gérer cela durant cette situation difficile que nous vivons tous.

Merci à toutes et à tous de vos questions, de vos retours. Je crois qu'il est important peut-être de voir s'il y a des personnes qui veulent prendre la parole au niveau audio. Est-ce que l'organisation peut envoyer des messages, est-ce qu'il peut y avoir un suivi sur les questions que nous envoyons ?

Donc est-ce qu'il y a d'autres mains de levées ? Je veux m'assurer qu'on a bien répondu à toutes vos questions pour Drew et Jonathan.

En tout cas j'aimerais remercier le personnel. Donc je pense que c'est une question pour nos présentateurs qui pourront y répondre plus tard.

Là c'est d'autres questions pour l'ICANN. Donc on va noter toutes les questions qui sont envoyées à l'ICANN et on va mettre ça sur la liste du CPWG, du groupe de travail, et nous allons donc vous répondre plus tard.

Et bien très bien, ces webinaires doivent servir de première étape pour les personnes qui veulent travailler au développement des politiques à l'ICANN et lutter contre l'utilisation malveillante du DNS.

Donc je crois qu'on a encore un petit de temps, si vous avez des questions ou des commentaires. Une question de Vivek, est-ce que le rapport DDAR a permis des actions proactives contre l'utilisation malveillante du DNS ? Donc, je ne sais pas si vous connaissez bien le système DDAR, Drew, je ne sais pas qui veut répondre à cette question…

JONATHAN ZUCK: Moi je crois que ce qui manque sur DDAR, sur ce système de signalement d'utilisation malveillante des noms de domaine, c'est qu'il est parfois difficile d'avoir beaucoup de données. Donc si on n'est pas au sein de l'ICANN, c'est difficile d'avoir beaucoup d'informations à partir de DDAR. Toutes les informations ne sont pas disponibles, je crois que ça ne va pas assez vite non plus avec le nom du bureau d'enregistrement qui est parfois accusé de fraude ou qui est frauduleux.

DREW BAGLEY : Oui, c'est tout à fait exact. Et lorsque vous voyez la révision de la CCT, et bien nous mettons l'accent là-dessus, je pense qu'il faut être basé sur plus de données pour régler ce problème et peut-être utiliser les données DDAR ou d'autres données parce que la communauté cybersécurité fait remonter beaucoup de données, donc on a besoin de mécanismes pour prendre des mesures rapidement.

JOANNA KULESZA : Merci beaucoup, Jonathan et Drew, de vos réponses. Je crois comprendre que c'est en effet une première étape vers le développement de politique. Donc je pense que le DDAR en effet, ce système DDAR, est une première mesure, mais peut être améliorée par l'ICANN. Et nous allons y travailler.

Donc il y a un rapport de feedback que nous aimerions avoir par rapport à ce webinaire, à l'utilité de ce webinaire, à la tenue de ce webinaire. Donc Yesim a des questions, je crois, à vous poser, nous allons lui donner la parole.

YESIM NAZLAR : Merci Joanna, de me donner la parole. Si vous permettez, j'aimerais que l'on passe à l'évaluation maintenant, nous avons des questions d'évaluation que nous allons maintenant vous présenter. Vous les avez à l'écran.

Comment avez-vous entendu parler de ce webinaire… Prenez quelques minutes pour répondre à ces questions, elles sont importantes. Je vais vous les lire également.

Comment avez-vous entendu parler de ce webinaire ? Choix multiple, questionnaire à choix multiple : Tweeter, Facebook, la liste de diffusion At-Large, le calendrier At-Large, par un collègue ou autre. Vous pouvez choisir autant de réponses que vous le désirez.

Je vais maintenant passer à la deuxième question. Dans quelle région vivez-vous ? Je vous les lis au cas où vous ne les voyez pas à l'écran. Donc l'Afrique, l'Asie Australie, îles Pacifiques, Europe, Amérique latine, Caraïbe, Amérique du Nord.

Troisième question. Comment était l'horaire du webinaire ? Vous vous rappelez que nous sommes à 15h UTC, est-ce que c'était une heure qui vous convenait ? Est-ce que c'était trop tôt ? Trop tard ?

Quatrième question. Est-ce que la longueur du webinaire, sa durée, était convenable ? Oui ou non. C'est une question oui ou non.

Cinquième question. La présentation était intéressante ? Vous êtes fortement d'accord, d'accord, pas d'accord ou en désaccord, tout à fait en désaccord ou pas.

Donc nous passons maintenant à la question suivante. J'ai appris quelque chose de ce webinaire ? Fortement d'accord, d'accord, neutre, en désaccord ou fortement en désaccord.

Et nous avons notre dernière question. J'aimerais participer à d'autres webinaires At-Large ? Fortement d'accord, d'accord, neutre, pas d'accord, absolument pas d'accord.

Je vais donc laisser ce sondage ouvert, comme ça vous aurez plus de temps pour y répondre et c'est donc la fin de l'évaluation, je redonne la parole à Joanna.

JOANNA KULESZA : Merci beaucoup Yesim, merci à toutes et à tous de vous être joint à ce webinaire, merci de vos réponses pour améliorer à chaque fois nos webinaires et indiquer votre intérêt pour ces webinaires.

Je ne pense pas qu'il y ait d'autres questions ou commentaires, donc nous allons conclure.

Le sous-groupe d'organisation des webinaires remercie toutes les personnes qui ont participé à l'organisation. Nous remercions nos intervenants, nous remercions Jonathan et Drew d'avoir pris du temps pour préparer tout cela, de nous parler du DNS qui est en constante mutation. Cela a été extrêmement intéressant pour travailler plus avant au développement de politique pour les utilisateurs finaux.

Donc vous avez acquis des connaissances et vous pourrez ainsi plus participer au développement des politiques de l'ICANN avec le groupe des politiques consolidées, groupe de travail. Nous aurons un webinaire le 1er juillet. Nous parlerons de cybersécurité en termes plus généraux, pas seulement d'utilisation malveillante du DNS. On parlera plus de géopolitique au 1er juillet, on parlera du rôle de l'ICANN au niveau géopolitique.

Je serai très heureuse de vous retrouver et de modérer ce webinaire le 1er juillet. Vous aurez plus d'informations d'ici là. Nous aurons plus de décisions du conseil d'administration d'ici là. Et l'ICANN nous aura donné plus d'informations sur les mesures prises. Donc je crois que c'est le 1er juin, le 1er juin ce webinaire, pas le mois de juillet, c'est au mois de juin. Vous aurez plus d'information sur ce webinaire qui se tiendra à 20h UTC.

Sans plus attendre, une nouvelle fois je remercie nos intervenants, nos participants, nos services linguistiques également qui nous ont soutenus. Merci à toutes et à tous.

YESIM NAZLAR : Merci de vous être joint à ce webinaire, nous levons maintenant la séance. Au revoir.

[FIN DE LA TRANSCRIPTION]