ICANN67 | Forum virtuel de la communauté – Séance de politique d'At-Large : Utilisation malveillante du DNS : un appel à l'action d'At-Large
Lundi 9 mars 2020 – 13h45 à 15h15 CUN

MICHELLE DESMYTER : Merci à tous pour votre patience. Nous allons commencer dans quelques minutes. Merci.

Bonjour à tous, bonsoir. Michelle DeSmyter, du personnel de l'ICANN. Bienvenue à la réunion virtuelle de l'ICANN67. Nous allons parler de l'utilisation malveillante du DNS. Nous sommes le 9 mars 2020, il est 18h45 UTC.

L'audio de la salle Zoom est en anglais. Vous pouvez utiliser les liens si vous souhaitez écouter en espagnol ou en français. Vous devriez avoir reçu avec votre invitation tous les liens. Les détails pour cette connexion se trouvent également sur la page wiki de l'ordre du jour de l'At-Large.

Nous ne ferons pas l'appel aujourd'hui pour des raisons de temps mais les dirigeants de l'At-Large et les participants seront notés.

Vous pourrez vos questions dans le chat en français, en espagnol ou en anglais en indiquant bien que c'est une question en marquant « *question* » ou « *comment* » pour commentaire. Tout sera traduit par écrit. Le personnel mettra des rappels de ce processus dans le chat de Zoom. Si vous êtes dans la salle Zoom, vous pouvez également lever la

main et le personnel vous donnera la parole pour poser votre question.

N'oubliez pas de donner votre nom lorsque vous parlez, non seulement pour la transcription mais également pour que les interprètes vous identifient. Veuillez parler clairement et lentement de manière à ce que l'interprétation puisse être faite.

Enfin, cette séance, comme toutes les activités de l'ICANN, est régie par le code de conduite de l'ICANN. Je vais mettre un lien dans le chat.

Et sans plus attendre, je passe la parole à Jonathan Zuck.

JONATHAN ZUCK : Merci à tous d'être présents. Nous avons 164-165 participants, donc c'est très bien.

L'ALAC a pris la décision de faire de l'utilisation malveillante du DNS un des sujets principaux de l'At-Large pour 2020. Donc l'idée de cette session, c'est de vous présenter d'une manière générale certains des sujets relatifs à l'utilisation malveillante du DNS. Il s'agira de notions de base pour certains, pour d'autres moins. Nous allons vraiment avoir une discussion de base sur l'utilisation malveillante du DNS, nous allons parler des enjeux auxquels nous sommes confrontés par rapport à l'augmentation de l'utilisation malveillante du DNS. Et nous allons lancer une campagne pendant l'année à venir à l'At-Large.

Dans l'ordre du jour, vous verrez qu'il y a des liens vers des vidéos de cette présentation ; elles sont en anglais, en espagnol et en français. Si

vous avez des problèmes pour vous connecter à Zoom, ces vidéos sont disponibles sur YouTube et vous pouvez regarder à partir des liens YouTube les vidéos. Si par exemple votre connexion Zoom n'est pas bonne, si vous avez des problèmes de bande passante ou si vous voulez y revenir par la suite, ces vidéos sont disponibles dans les différentes langues et vous avez des liens sur l'ordre du jour.

Ce que nous allons faire, c'est que nous allons vous donner la version en anglais de la vidéo et nous aurons la traduction instantanée sur Zoom. Mais n'hésitez pas à utiliser les liens sur l'ordre du jour pour regarder la vidéo sur YouTube si c'est plus facile pour vous.

Donc sans plus attendre, je vais demander au personnel de lancer la vidéo. C'est parti.

[VIDÉO] : Bonjour, bonsoir et pour ceux qui ont moins de chance, bonne nuit.

L'élaboration des politiques de l'ICANN est d'une grande complexité étant donné la mission relativement simple de l'organisation. Il est facile de passer à côtés des gros problèmes lorsqu'on est plongés dans les petits. En tant que seul représentant des intérêts des utilisateurs finaux, il est critique de ne pas perdre notre objectif de vue. Nous devons identifier les principaux problèmes auxquels sont confrontés les utilisateurs individuels afin d'apporter des solutions.

Peut-être que la menace la plus importante pour les utilisateurs finaux, c'est celle de l'utilisation malveillante du DNS. Nous allons

donc parler de cette utilisation malveillante du DNS de manière à ce que cela fasse partie de la conversation que nous avons dans la communauté de l'ICANN.

De plus en plus à l'At-Large, nous allons demander les uns aux autres : « Que faites-vous par rapport à l'utilisation malveillante du DNS ? »

De quoi s'agit-il ? L'utilisation malveillante du DNS, c'est un terme qui est souvent utilisé dont on a largement débattu au sein de l'ICANN en fait après la révision sur la concurrence, le choix et la confiance du consommateur. Le Conseil a lancé une nouvelle initiative communautaire pour définir l'utilisation malveillante du DNS dans le but de concevoir un meilleur plan d'attaque.

Même quand la définition est conservatrice, nous pouvons commencer à concevoir un cadre pour lutter contre l'utilisation malveillante du DNS et l'appliquer plus souvent dans la mesure où la définition est élargie.

Nous connaissons tous assez bien le DNS, le système de noms de domaine. C'est un système sophistiqué de questions et de réponses qui vous permet de vous rendre là où vous voulez sur le web et c'est un peu comme une chasse aux trésors où vous allez demander à une personne le nom de la personne qui connaît le numéro de celle que vous souhaitez joindre.

Bien sûr, comme on le dit dans les films, toutes ces questions peuvent vous amener à être remarqué par les mauvaises personnes. Demandez à Dorothée, elle cherchait le Magicien d'Oz.

Autrement dit, l'utilisation malveillante du DNS est une attaque où l'utilisation du DNS est faite 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 en ce qui nous concerne, nous allons parler de l'emploi abusif du DNS ou utilisation malveillante du DNS.

L'une des attaques les plus connues, c'est le DDoS. Ici, vous avez un délinquant qui utilise un réseau d'ordinateurs zombies pour envoyer une telle quantité de requêtes que le serveur est surchargé.

Parfois, un élément criminel s'interpose entre vous et les serveurs auxquels vous demandez des informations. Cela est possible à travers une attaque dite de l'homme du milieu ou alors d'une attaque de type empoisonnement du cache du DNS. Autrement dit, vos requêtes sont interceptées et vous recevez le mauvais numéro en réponse.

Ces redirections du côté des serveurs peuvent être utilisées pour quelque chose que l'on appelle le hameçonnage. Vous êtes redirigé vers un site qui ressemble à celui que vous vouliez atteindre mais qui est configuré en fait pour prendre vos identifiants de connexion. Vous pensez que vous vous connectez à une banque mais en réalité, vous remplissez simplement un formulaire pour que les pirates puissent accéder à votre compte.

Un des abus les plus courants effectués à travers le DNS est le hameçonnage et une manière beaucoup moins complexe de vous amener sur le mauvais serveur est simplement de vous demander d'y

aller. Dans ce cas, vous recevez un courriel suggérant qu'il y a un problème avec votre compte de banque et que vous devez vous connecter pour régler le problème.

Cependant lorsque vous cliquez sur le lien, vous êtes redirigé vers un site de déploiement. Ce processus est appelé hameçonnage parce que vous êtes attiré vers le site frauduleux. Voici un exemple de ce qu'un tel courriel pourrait dire. Vous pouvez voir qu'il y a des éléments clés dans ces courriels, une sorte de crise avec un remède à court terme de manière à ne pas provoquer beaucoup de réflexion. Bien sûr, les courriels ne sont pas le seul moyen utilisé ; parfois, il y a des pièces jointes contenant des logiciels malveillants

Un point particulièrement préoccupant pour l'At-Large, c'est celui des noms de domaine internationalisés ou IDN, c'est-à-dire les noms de domaine utilisant des caractères non latins. Ces domaines relativement nouveaux sont essentiels pour attirer le prochain milliard d'utilisateurs de l'internet. Environ 70 % du monde utilise des alphabets de noms latins et en 2012, nous avons pu enregistrer différentes langues telles que le russe, l'arabe et le chinois.

Naturellement, chaque nouvelle innovation entraîne des innovations correspondantes de la part des délinquants et c'est le cas des IDN. Il s'avère qu'un bon nombre de lettres des alphabets non latins ressemblent étrangement à des lettres de l'alphabet latin. Qui savait qu'il y avait tant de façons d'écrire Bank of America ? Lorsque quelqu'un voit une de ces orthographes tout en lisant rapidement un courriel, qu'est-ce qui l'empêcherait d'y cliquer ?

En plus de collecter vos informations d'identification, ces courriels et sites web frauduleux ont pour objectif principal d'implanter des logiciels sur votre ordinateur. Ces logiciels sont généralement appelés logiciels malveillants. Mais il en existe de nombreuses variétés. Vous avez déjà entendu parlé de ce type de programmes et bon nombre d'entre vous, vos familles, vos amis, en ont sûrement été victimes.

Nous n'allons pas rentrer dans le détail de ceci aujourd'hui mais ce que l'on peut dire, c'est qu'il s'agisse de logiciels espions ou de rançonlogiciels, vous n'en voulez pas dans votre ordinateur. Malheureusement, les infections de logiciels malveillants sont en augmentation. Au cours des 10 dernières années, les infections par logiciels malveillants aux augmenté de près de 700 %. À titre d'exemple, les attaques de rançonlogiciels ont augmenté de 350 % en 2018 uniquement.

En particulier après la révision de la concurrence, du choix et de la confiance des consommateurs de la série de TLD de 2012, le département en charge de la conformité contractuelle de l'ICANN a fait de son mieux. Il y a eu beaucoup de données publiées plus précises sur les plaintes de manière à rendre le processus de révision un peu moins aléatoire.

Mais cela ne suffit toujours pas. Vous avez peut-être entendu parler de quelque chose que l'on appelle le DAAR ou le système de signalement des cas d'utilisation malveillante des noms de domaine. Les rapports mensuels fournissent juste assez de données pour savoir qu'il y a un problème. Ils n'en fournissent pas assez pour en faire quelque chose

comme éviter un domaine ou un bureau d'enregistrement qui ne semble pas honnête.

Cependant, en utilisant le DAAR, nous pouvons déterminer le pourcentage de cas d'utilisations malveillantes détectés et celui-ci a diminué de moins de 1 % depuis sa création. On peut donc convenir que l'abus du DNS est un problème majeur pour les utilisateurs individuels.

Mais que peut faire l'At-Large ? L'At-Large adoptera une approche à deux volets pour lutter contre l'utilisation malveillante du DNS, la sensibilisation et l'élaboration des politiques à l'ICANN. L'At-Large élaborera du matériel éducatif pour les utilisateurs finaux de manière à mieux les protéger contre l'utilisation malveillante du DNS. L'At-Large a une structure unique qui lui permet de diffuser des informations aux organisations régionales At-Large, les RALO, qui à leur tour peuvent distribuer ces documents aux structures At-Large qui les composent et qui ont elles-mêmes des membres individuels auxquels elles peuvent distribuer le matériel. L'At-Large développe ce réseau depuis des années et quoi de mieux que de protéger les utilisateurs contre les criminels sur internet. Il y a un certain nombre de messages que nous pouvons transmettre pour aider les gens à éviter des pièges qui leur sont tendus au jour le jour.

L'ironie, c'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 sociaux intelligents. En bref, s'ils veulent votre

mot de passe, ils vous le demandent, tout simplement. C'était vrai avant l'internet et cela est toujours vrai.

L'At-Large doit éduquer les utilisateurs, être à l'affût de nouvelles qui sont trop bonnes ou trop mauvaises pour être vraies. Et il existe des moyens de le faire. Il est toujours possible de savoir si un courriel est frauduleux ou pas.

Nous aimons nous moquer de ces courriels d'hameçonnage en raison de leurs fautes de grammaire mais ce que nous ne savons, c'est que ces fautes sont intentionnelles puisque celles-ci déclenchent simultanément la suppression de la part de ceux qui reconnaissent l'arnaque et de la compassion chez ceux qui sont moins sophistiqués. L'At-Large peut certainement aider les utilisateurs à discerner l'authenticité d'un courriel inattendu.

Cela va sans dire mais l'At-Large le dira quand même, les utilisateurs individuels devraient avoir un logiciel de protection anti-virus sur leur PC et sur leurs appareils portables. De fait, aux États-Unis où l'on s'attendrait à une sophistication considérable de la part des utilisateurs, près de 50 % des ordinateurs ne sont pas protégés contre les virus. L'At-Large doit encourager les utilisateurs finaux à demander à leurs employeurs s'ils ont des serveurs compatibles avec le DNSSEC pour prévenir les événements telles que les attaques de l'homme du milieu.

Par ailleurs, l'At-Large doit se faire entendre dans les couloirs, les réunions et les conférences téléphoniques qui intègrent le processus

d'élaboration de politiques de l'ICANN. L'At-Large participera à l'élaboration de politiques de l'ICANN à chaque étape du processus, que ce soit une conversation dans un couloir ou la participation à un groupe de travail ou à une équipe de révision. Et nous nous impliquerons activement à la plaidoirie pour des réformes, à la fois au sein de l'ICANN et auprès des entreprises qui servent les utilisateurs finaux. Donc si quelqu'un nous pose une question sur la météo, nous dirons : « La température ressentie suggère une utilisation malveillante du DNS. »

Heureusement, nous ne sommes pas seuls. La majorité de la communauté de l'ICANN se préoccupe de l'utilisation malveillante du DNS et hésite à autoriser une nouvelle série de TLD sans réforme. Il n'est pas possible qu'une minorité soit en mesure de lancer l'ICANN vers une nouvelle série sans la véritable adhésion du reste de la communauté. L'At-Large s'est associée avec d'autres groupes pour sonner le signal d'alarme concernant l'utilisation malveillante du DNS et pour promouvoir activement une réforme.

Notre première tâche est de maintenir une position. Aucune nouvelle série ne devrait pouvoir être lancée sans 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. Il ne peut pas simplement réagir aux plaintes mais il doit pouvoir utiliser son pouvoir de supervision pour reconnaître le pourcentage élevé d'utilisation malveillante du DNS.

Il nous fait limiter le nombre d'enregistrements parce qu'il y a un lien avec l'utilisation malveillante du DNS. Bien sûr, il existe des utilisations légitimes pour les enregistrements groupés mais l'At-Large continuera de plaider pour une vérification accrue d'une telle activité en exigeant peut-être une notification en tant que titulaires légitimes.

L'équipe de révision de la CCT, 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. L'At-Large continuera de travail dans ce sens. 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 désormais affecté est de 20 millions de dollars pour justement s'occuper de la sécurité et de la stabilité du DNS.

Il y a 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 en engagement envers les meilleures pratiques. C'est génial. 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 l'At-Large ne doit pas baisser les bras non plus.

C'est un peu comme cette BD de Dilbert qui nous rappelle qu'une fois que tout le monde a adopté les meilleures pratiques, ces nouvelles pratiques deviennent la norme et ne sont plus les meilleures. Les délinquants ne sont pas satisfaits de la situation et nous ne voulons

pas non plus nous permettre de l'être. Même les gentils peuvent mieux faire.

Tout cela pour dire qu'il s'agit d'une crise dont 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 le .eu montre une précision de près de 80 % dans ces prévisions.

En fin de compte, il n'y a vraiment qu'une seule unité constitutive, celle des utilisateurs finaux. C'est pour protéger les intérêts de ces utilisateurs finaux qu'At-Large a été créée. L'utilisation malveillante du DNS les affecte tous. Reconnaissons-le, nous n'avons pas aucun intérêt à ce que le DNS soit utilisé à des fins malveillantes.

Vous pouvez vous rendre sur atlarge.wiki/dnsabuse pour davantage d'informations. Merci beaucoup.

[FIN DE LA VIDÉO]

Merci à tous d'avoir bien regardé cette présentation. Nous allons vous envoyer cette page sur l'utilisation malveillante du DNS. Nous allons avoir une page sur le site où vous pourrez trouver toutes les ressources. Vous aurez cette vidéo et vous pourrez la revoir en français, en anglais ou en espagnol. Il y a aussi la version YouTube de ces vidéos qui est disponible.

Maintenant, je voudrais ouvrir la conversation et recevoir des votre part des questions ou commentaires si besoin est. Alan Greenberg, allez-y.

ALAN GREENBERG : C'est un bon exemple de ce que l'on attend de l'ICANN depuis longtemps. Je suis très heureux de voir que nous avons pris la tête des travaux et de la démarche. Merci.

JONATHAN ZUCK : Volker, voulez-vous prendre la parole ?

VOLKER GREIMANN : Oui. Je pense que c'est un bon effort de travailler contre l'utilisation malveillante du DNS. On en a parlé depuis la dernière réunion de l'ICANN, nous avons parlé de ce cadre de travail sur l'utilisation malveillante du DNS – dnsabuseframework.org. C'est un site qui détaille le nombre d'opérateurs de registre et de bureaux d'enregistrement qui font face à ces cas d'utilisation malveillante du DNS. Et là, vous pouvez avoir les détails sur tout cela. Merci.

Merci d'avoir donné des détails sur toutes ces choses auxquelles nous faisons tous les jours chacun d'entre nous.

JONATHAN ZUCK : Merci Volker. Et merci au groupe des bureaux d'enregistrement et de opérateurs de registre qui ont signé à ces meilleures pratiques et ceux

qui le font déjà. Je ne connaissais pas ce nouveau site .org dont vous venez de nous parler, dnsabuseframework.org. Nous allons tous aller voir cela.

Je l'ai mentionné brièvement durant la séance, il y a des bureaux d'enregistrement et opérateurs de registre qui font beaucoup plus d'efforts que d'autres pour combattre cette utilisation malveillante du DNS. Nous voulions vraiment souligner cela. Le problème reste avec les mauvais acteurs. Il nous faut soulever ces problèmes avec ces TLD ou de ces opérateurs de registre. Nous savons qu'il y a un problème. Le problème, c'est comment pouvons-nous faire face à ces mauvais acteurs ? Cela pose bien sûr une charge supplémentaire aux bons acteurs.

Avec cette utilisation malveillante qui augmente, il est important de pouvoir faire des efforts importants. Nous espérons voir encore de meilleures pratiques ou de bonnes pratiques de votre part. Je vous remercie tous et nous, l'ICANN, nous allons essayer de faire un meilleur travail pour faire face à ces mauvais acteurs.

NATALIE : Est-ce que vous pouvez nous donner des recommandations sur le sujet par rapport à ICANN Learn ?

JONATHAN ZUCK : Oui Natalie. Je pense que c'est une bonne idée, c'est quelque chose dont nous avons déjà parlé. Nous allons voir quelle sorte de plan de

sensibilisation nous pourrions utiliser. Peut-être pourrions-nous avoir un site web dédié pour les utilisateurs finaux. L'ironie dans tout cela, c'est que l'éducation pourrait jouer un rôle énorme pour atténuer les choses parce qu'il s'agit de gens qui trichent avec d'autres personnes. Vous savez, ce sont des gens qui essaient de tromper les gens pour obtenir leurs mots de passe, leurs informations, etc. Donc il faut continuer à travailler sur cela et ICANN Learn pourrait aider, bien sûr.

Je vais passer la parole maintenant à Joanna qui, en ce moment, travaille sur un cours sur l'élaboration des politiques avec ICANN Learn. Peut-être qu'elle pourra vous donner plus de détails. Joanna, voulez-vous prendre la parole ?

JOANNA KULESZA : Je suis très heureuse de voir que nous avons beaucoup de participation. J'attends vraiment vos commentaires, vos informations dans le chat. Je considère ces séances comme des séances de sensibilisation aussi, donc si vous avez des questions, posez-les.

Nous travaillons à ICANN Learn sur un cours qui donne des informations sur l'élaboration des politiques à l'ICANN. L'utilisation malveillante du DNS est sur notre ordre du jour. Nous voulons à ICANN Learn fournir un cours qui discuterait de cette utilisation malveillante mais nous voulons aussi nous assurer que le langage utilisé soit compréhensible. Cet acronyme de l'utilisation malveillante du DNS est déjà un acronyme. Donc nous voulons nous assurer que tout cela sera très compréhensible sur le site, des informations faciles à digérer.

Je vois qu'il y a là un bon potentiel. Nous allons pouvoir transposer la présentation de Jonathan sur ce site et dans le cours. Nous pensions que nous pouvons incorporer cela dans le cours d'ICANN Learn. Il y aura d'autres ressources qui seront mises à disponibilité. La communauté travaille de façon très proche avec toutes les RALO pour pouvoir adresser les questions ou les besoins au niveau régional.

Voilà donc le plan général lorsqu'il s'agit de sensibilisation. Il s'agit de fournir de nouvelles ressources dans ce cours d'ICANN Learn. J'attends vos informations, vos commentaires. Contactez-moi ou Alfredo ou rejoignez-nous sur un de nos appels.

Merci beaucoup.

JONATHAN ZUCK : Merci Joanna. Bien sûr, nous espérons recevoir des commentaires parce qu'à travers ces messages, nous pouvons atteindre plus de personnes. Cela pourrait être un module d'un cours qu'on développe en ce moment, un cours adressé à un public plus général et cela se passe en interne.

Natalie, vous avez levé la main mais est-ce que c'était tout à l'heure ou est-ce que c'est maintenant ?

NATALIE : Je dois baisser la main, excusez-moi.

JONATHAN ZUCK : Russ.

RUSS MUNDY : Comme vous savez, je fais la promotion du DNSSEC depuis longtemps et je suis très heureux de voir que ce DNSSEC était inclus dans votre présentation. Il s'agit là d'un aspect des compétences qui vont nous permettre d'atténuer l'utilisation malveillante du DNS.

Le texte, du moins les mots autour du DNSSEC encourageaient les gens à demander à leur employeur d'utiliser le DNSSEC. C'est bien, toutes les sociétés, les organisations, les employeurs devraient faire cela. Mais il est aussi important de noter, surtout au niveau de la perspective de l'ALAC, qu'il est approprié de demander aux personnes, aux ISP, de fournir ce genre de services conformes au DNSSEC. Les ISP eux-mêmes doivent signer leur zone pour que le hameçonnage soit plus compliqué et pour que les attaques de l'utilisation malveillante soient moins faciles.

Je ne suis pas dans la salle DNSSEC mais je pense que malgré tout, le DNSSEC peut apporter beaucoup lorsqu'il s'agit d'utilisation malveillante du DNS.

Mais vraiment, votre présentation était une des meilleures présentations que je n'aie jamais vues sur l'utilisation malveillante du DNS.

JONATHAN ZUCK : Très bon commentaire. J'essayais de penser à ce que je pouvais conseiller aux utilisateurs finaux. C'est une bonne suggestion de votre part. Alors que nous développons ces ressources pour les utilisateurs finaux, nous allons prendre en compte ce point de vue et nous allons remettre cela dans notre appel à l'action. Merci d'avoir apporté ces informations.

Ephraim.

EPHRAIM KENYANITO : Il y a une chose qui a été mentionnée tout à l'heure, vous avez mentionné les bureaux d'enregistrement. Est-ce que vous pouvez donner plus de détails ?

JONATHAN ZUCK : Vous avez dit quoi ? Quels bureaux d'enregistrement font quoi ?

EPHRAIM KENYANITO : Vous avez parlé de la détection automatique de l'utilisation malveillante du DNS, donc de toutes ces activités.

JONATHAN ZUCK : C'est .eu qui est à la tête de cela. Je pense que .uk aussi a commencé à expérimenter sur le sujet. Il y a aussi un papier blanc qui a été publié sur l'expérimentation qui a été faite pour .eu sur la méthodologie et le succès et la réussite de ce qu'ils ont fait avec ces analyses et ces prédictions. Je peux m'assurer de mon côté que cette information soit

rajoutée sur l'ordre du jour ou du moins quelque part où vous pourrez trouver ces informations. Mais il y a vraiment un papier blanc qui a été publié par .eu sur ces efforts sur les analyses de prédiction qui sont très intéressantes. On peut trouver ces informations et on peut aussi utiliser cela en exemple pour que l'on puisse mettre en œuvre des meilleures pratiques. C'est vraiment une bonne chose qui a été faite, encore une fois des grands acteurs, des acteurs positifs qui ont fait du travail sur l'utilisation malveillante du DNS.

EPHRAIM KENYANITO : Il s'agit de ces deux bureaux d'enregistrement ? Ou est-ce que cela a été fait aussi en Asie ou d'autres régions ?

JONATHAN ZUCK : Si j'ai bien compris, il s'agit seulement de ces deux bureaux d'enregistrement. Mais je pense que les recherches sont en cours à .eu. Mais il y a aussi des recherches sur l'apprentissage des machines qui sont en cours en Asie. Si vous m'envoyez un courriel, je partagerai ces informations avec vous. Nous avons fait référence il y a peu de temps dans des commentaires sur ICANN Org le jour de la Saint-Valentin, je me souviens, on y avait fait référence. Donc vous devriez trouver ces informations sur cette page du 14 février. Ce n'est pas la même chose que lorsqu'on parle du mécanisme de prévision de l'utilisation malveillante du DNS. Ces informations viennent de l'Asie. Ce sont les deux bureaux d'enregistrement dont j'ai connaissance.

LAUREEN KAPIN : Je parle en mon propre nom. Je suis avocate à la Commission américaine du commerce sur la protection du consommateur.

Le site ftc.gov a des ressources très intéressantes et cela inclut des documents qui vous donnent des informations afin de pouvoir éviter les attaques d'hameçonnage, etc. Ce sont des documents qui sont disponibles en espagnol et en anglais. Et si votre organisation veut utiliser ces ressources et utiliser son propre logo sur ces mêmes ressources, nous pouvons faciliter cela. C'est du matériel éducatif écrit par des experts. Ils utilisent un langage qui est facile à comprendre pour tous. Même si l'anglais et l'espagnol ne sont pas les langues maternelles, c'est du matériel très efficace.

JONATHAN ZUCK : Merci pour cette contribution. Peut-être que vous pourriez afficher l'URL dans le chat. Et je pense qu'effectivement, les gens pourront trouver ceci utile. Et nous allons effectivement utiliser votre idée et votre proposition de refaire les marques.

L'At-Large a un avantage en fait par rapport à d'autres unités constitutives puisqu'il y a un cadre de travail de participants de différents organismes. Vous savez, il y a les organisations régionales de l'At-Large, il y en a cinq : l'Amérique du Nord, l'Afrique, l'Europe, l'Amérique latine et l'Asie-Pacifique. Dans chacune de ces organisations, il y a des centaines de ce que l'on appelle les structures At-Large qui souvent sont des organisations à but non lucratif ainsi que des personnes, des individus qui sont membres des RALO.

Nous allons un petit peu utiliser la pyramide de contacts pour contacter les utilisateurs finaux et leur envoyer ces supports. Effectivement, quand il y a des supports qui sont utiles du type de ce que vous avez mentionné, nous les ferons suivre. Nous utilisons notre réseau pour diffuser les informations.

Marita Moll, allez-y.

MARITA MOLL : Merci.

Excellente vidéo. Je pense qu'elle permettra d'informer des personnes qui ont déjà certaines connaissances. En fait, il y a différents niveaux de connaissance et il y a beaucoup de personnes qui doivent être informées par rapport à ce sur quoi il faut ne pas cliquer.

Je crois qu'il y a des choses que nous pouvons faire pour nous assurer que ces messages n'atteignent personne. Je crois qu'il y a déjà les processus à mettre en place pour éviter que ces messages arrivent chez notre voisin, même si on est tous un petit peu parfois pris de cours.

JONATHAN ZUCK : Très bien, Marita. En fait, cette vidéo, ce n'est pas celle que l'on va utiliser pour les utilisateurs finaux. Nous allons créer d'autres supports. Cette vidéo était vraiment à l'intention des participants de l'At-Large de manière à lancer la campagne de l'utilisation malveillante du DNS comme sujet au sein de l'At-Large.

Ephraim, vous avez une autre question ou c'est une ancienne main ?

EPHRAIM KENYANITO : Excusez-moi, c'était une ancienne main. Je la baisse.

JONATHAN ZUCK : Pas de problème.

Mason, allez-y.

MASON COLE : Bonjour Jonathan. Merci de me donner la parole.

Je vous félicite d'abord pour cette vidéo qui est excellente. Je souhaitais aussi attirer l'attention de l'ALAC sur la BC et son travail dans le domaine de l'utilisation malveillante du DNS depuis six mois.

Nous avons publié une déclaration depuis la réunion de Montréal ; vous pouvez la voir sur notre site web. Je peux même mettre le lien dans le chat.

Ensuite, il y a eu un échange entre la BC et le Conseil d'Administration de l'ICANN sur le sujet de ce que l'on peut faire avec les parties contractantes pour s'occuper de l'utilisation malveillante du DNS.

Donc j'attire l'attention de l'ALAC là-dessus. J'aimerais vous demander votre soutien, si vous le voulez bien. Et je vous encourage à être beaucoup plus impliqué dans l'organisation de manière à faire avancer la discussion sur l'utilisation malveillante du DNS.

JONATHAN ZUCK : Très bien, merci. Effectivement, nous serons très heureux de travailler avec vous. Nous avons pu voir certains de vos commentaires, nous savons que vous avez des membres individuels qui sont très impliqués dans la protection des clients. Effectivement, je crois qu'il y a beaucoup de points communs sur lesquels nous pouvons coopérer avec l'unité constitutive des utilisateurs commerciaux.

MICHELLE DESMYTER : Nous avons un commentaire. Je vais le lire. Le commentaire, c'est : « L'ICANN a des formulaires web pour le WHOIS et pour tout ce qui est plaintes d'inexactitude, qui sont difficiles à vérifier. Il s'agit du temp.spec/RGPD. Est-ce que l'ICANN pourrait fournir un moyen de signaler les utilisations malveillantes sur le site web, le hameçonnage, etc. ? » J'ai mis ce lien dans le chat.

JONATHAN ZUCK : Je ne vois pas le lien dans le chat mais c'est parce qu'il est peut-être monté trop haut. Effectivement, nous allons réfléchir à ces possibilités. Le WHOIS commence à être quelque chose qui prend une nouvelle forme suite au RGPD et suite aux efforts du EPDP. Mais nous continuons de nous concentrer du point de vue des politiques sur l'automatisation maximale du processus de manière à ce que les agences de protection aient accès aux données pour pouvoir fournir les services qu'ils fournissent dans la lutte contre l'utilisation malveillante du DNS.

MICHELLE DESMYTER : Jonathan, il y a une autre question de Ram Mohan : « Est-ce qu'il s'agit principalement d'une question d'hygiène que l'on devrait traiter de manière similaire à ce que l'on fait dans la vie quotidienne, donc se laver les mains, etc. en gros installer un filtre anti-spam, ne pas se toucher le visage, ne pas cliquer sur les liens aléatoires, etc. ? »

JONATHAN ZUCK : Oui, c'est vrai que c'est un petit peu une question d'hygiène.

Il y a différents types d'utilisations malveillantes de l'infrastructure du DNS qui ne sont pas des questions d'hygiène ou qui ne peuvent pas être maîtrisées par les utilisateurs. Et là, les DNSSEC entrent en jeux. Les attaques de l'homme du milieu, ce sont des choses qui ne peuvent pas être vraiment maîtrisées par les utilisateurs finaux. Mais il y a beaucoup de choses que les internautes peuvent faire si on les éduque : augmentation de la friction sur les enregistrements en gros, il y a différents moyens analytiques qui pourraient améliorer les choses pour les utilisateurs finaux.

Nous avons tous l'habitude de cliquer sur ce qui nous est familier donc si vous voyez quelque chose qui dit Bank objectif America mais qu'une des lettres n'est pas exactement similaire à ce qu'elle devrait être et qu'il s'agit d'un IDN, il est parfois un petit peu difficile de décider, même pour l'utilisateur final qui s'y connaît bien, de savoir s'il peut cliquer ou pas. Être impliqué dans la communauté du DNS et éduquer

les consommateurs, les utilisateurs finaux, je pense que cela pourra contribuer à atténuer l'utilisation malveillante du DNS.

Y a-t-il d'autres questions ? Très bien.

J'avais essayé de réfléchir à des manières intéressantes de gérer cette réunion uniquement virtuelle ; je souhaitais que ce soit plus intéressant. Donc la suite à l'ordre du jour, c'est en fait un questionnaire qui va nous aider à renforcer nos connaissances sur ceci. Vous pouvez jouer, vous pouvez utiliser votre téléphone, votre ordinateur portable. Pas besoin d'utiliser d'application particulière. Vous allez sur atlarge.wiki/daquiz. Vous devriez pouvoir simplement cliquer sur ce lien et utiliser votre navigateur. Vous pouvez utiliser votre téléphone, votre tablette, votre ordinateur pour répondre. Vous allez à atlarge.wiki/daquiz. Je crois que quelqu'un l'a mis dans le chat, c'est très bien. Je vais donc lancer ce questionnaire. Je vous donne une seconde pour vous préparer et ensuite, je vous donnerai une minute pour répondre aux questions. Et nous lancerons le questionnaire dans un instant. Attendez, je réfléchis un instant à ce que je fais.

Je n'avais pas allumé mon micro. Je m'excuse.

Est-ce que tout le monde a bien vu le quiz que j'ai mis à l'écran ?

MICHELLE DESMYTER : Oui, ça va Jonathan.

JONATHAN ZUCK : Je vous laisse encore un petit moment pour que vous puissiez vous enregistrer. Vous allez voir des questions avec des choix multiples. Vous avez quelques secondes pour répondre et on vous montrera ensuite la réponse à la question avant de passer à la prochaine question. Je pense que nous avons des personnes qui sont prêtes à démarrer. Je m'excuse encore d'avoir éteint mon micro. Je vous donne encore un petit moment et nous allons commencer.

Quelqu'un veut-il que je lise ces questions ou est-ce qu'on peut laisser les participants les lire à même l'écran ? J'aurais dû certainement trouver une manière d'incorporer une musique dans ma présentation.

SÉBASTIEN BACHOLLET : Jonathan, comme vous voyez, nous sommes 200 et quelques personnes en ligne et vous avez 60 réponses. Ce n'est peut-être pas une bonne utilisation de notre temps.

JONATHAN ZUCK : Merci Sébastien. C'est juste une expérimentation.

SÉBASTIEN BACHOLLET : Oui, mais une expérimentation pour 200 et quelques personnes, ce n'est pas forcément facile.

ALAN GREENBERG : Ceux qui ne répondent pas ne peuvent pas s'amuser en répondant aux questions avec les mauvaises réponses.

ORATEUR NON-IDENTIFIÉ : Qu'est-ce qu'un « maleware » ?

JONATHAN ZUCK : C'était une erreur de ma part.

ALAN GREENBERG : Je pense que vais vous intenter un procès.

ORATEUR NON-IDENTIFIÉ : Je pensais que ce n'était pas une erreur et que c'était intentionnel.

ALAN GREENBERG : C'était tout à fait intentionnel. Je pense que la première réponse est la bonne réponse ici.

ORATEUR NON-IDENTIFIÉ : Quel bouton correspond au « maleware » ?

ORATEUR NON-IDENTIFIÉ : Taisez-vous.

ALAN GREENBERG : Encore, c'est l'homme au milieu. Je pense qu'ils ont quelque chose contre nous.

ORATEUR NON-IDENTIFIÉ : Alan, quel est votre mot de passe ?

ORATEUR NON-IDENTIFIÉ : Ça fonctionne. C'est surprenant mais cela fonctionne souvent comme cela.

JONATHAN ZUCK : Merci à tous pour votre participation à cette petite expérimentation. Il s'agit de la version virtuelle de l'ICANN donc il faut qu'elle soit un peu plus interactive et un peu plus amusante.

Une autre chose que j'aimerais faire aussi alors que nous clôturons la séance, c'est de vous parler des autres séances sur l'utilisation malveillante du DNS cette semaine. Il y a une séance sur les outils holistiques pour la conformité. C'est une bonne séance où participera une personne responsable des politiques pour GoDaddy. Ils vont observer différents scénarios et voir quelle serait la meilleure manière pour le département de la conformité pour faire face à ces différents scénarios. Nous allons obtenir l'opinion de ces experts et ainsi, peut-être que nous pourrons tirer de nouvelles informations de cette conversation, à savoir si le département de la conformité a tous les outils nécessaires pour lutter contre l'abus ou l'utilisation malveillante systémique. On va donc discuter de tout cela durant cette séance.

Ensuite, il y a une autre séance dont j'aimerais que Joanna nous explique un peu en quoi cela retourne. Parlez-nous un peu de la conversation que vous allez tenir lors de votre séance.

JOANNA KULESZA : Notre séance de mercredi où nous parlerons de la cybersécurité et du cybercrime est liée à la discussion sur l'utilisation malveillante du DNS. J'apprécie la possibilité de travailler dans ce sens avec Jonathan qui a un avis très orienté vis-à-vis de la conformité.

Ce qu'on essaie de faire durant la séance au niveau de « One World, One Internet », nous voulons aussi parler de la cybersouveraineté, à savoir si la mission de l'ICANN pourrait correspondre à cette discussion.

Veni Markovski va nous rejoindre. Il y a publié un rapport sur la cybersécurité, sur le cybercrime. León aussi a accepté de nous rejoindre. Patrik Fältström va nous donner un historique au niveau technique. Nous allons aussi avoir la participation du NCUC et on parlera de la cybersouveraineté dans l'espace internet.

Et bien sûr, nous allons utiliser l'approche de Jonathan sur la conformité contractuelle et nous parlerons de tout cela durant la séance de mercredi. Nous essayons d'étudier les choses sur un aperçu un peu plus large pour voir ce qu'il y a sur l'ordre du jour du Conseil d'Administration pour les cinq années à venir.

Nous voulons aussi faire le lien entre les discussions qui ont lieu en dehors de la bulle ICANN. Cela est important pour les utilisateurs finaux lorsqu'il s'agit de leur sécurité.

Comme je l'ai déjà dit brièvement dans le chat, nous aimerions aussi explorer cette question de l'utilisation malveillante du DNS et de son lien vis-à-vis des intérêts des utilisateurs finaux. Il faut parler de la sécurité en ligne, nous voulons aussi explorer les liens entre les cybercrimes et la cybersécurité, l'abus du DNS et bien sûr tout ce qui concerne la confidentialité, etc. Nous allons aussi parler du rôle de l'ICANN au niveau des politiques en ce qui s'agit d' « Un monde, un internet. »

Merci de m'avoir laissé présenter ma prochaine séance. Merci Jonathan pour cette introduction fantastique sur l'utilisation malveillante du DNS. J'espère que nous allons pouvoir contribuer au débat au sein de l'ICANN mais aussi en dehors de l'ICANN pour tout ce qui est relatif à la cybersécurité.

Merci.

JONATHAN ZUCK : Merci Joanna. J'attends avec impatience votre séance. C'est une grosse séance intercommunautaire, donc j'espère que nous aurons autant de participants qu'on aurait eus à Cancún. J'espère que tout le monde viendra.

Puis un petit peu plus tard dans la journée, nous aurons une session sur la conformité.

Chers membres du personnel, je crois que c'est tout ce que j'avais à dire, sauf s'il y a des questions dans le chat.

MICHELLE DESMYTER : Un instant Jonathan. Je ne crois pas, mais je vérifie. Non, il n'y a pas d'autres questions.

JONATHAN ZUCK : Merci à tous d'avoir participé, merci Volker d'avoir mentionné le nouveau site. Regardez tous ce nouveau site, dsnabuseframework.org. Et à la fin de la vidéo, vous avez le site web pour aller voir, atlarge.wiki/dnsabuse. Allez-y, allez regarder ce qu'il y a sur cette page sur le site de l'At-Large.

Merci à tous ceux qui ont participé. C'était très intéressant. Merci à tous.

MICHELLE DESMYTER : Merci Jonathan, merci à tous. La réunion est terminée. Merci à tous.

[FIN DE LA TRANSCRIPTION]