DEVAN REED : Bonjour à tous, bonsoir, bienvenue à cet appel d'AFRALO, ce webinaire sur la sécurité des données en ce mardi 7 septembre 2021 à 18 h 30 UTC.

Nous ne ferons pas l'appel puisqu'il s'agit d'un webinaire, mais les participants sont enregistrés sur Zoom.

Nous avons l'interprétation aujourd'hui avec Jacques et Isabelle en Français.

Du personnel nous avons Silvia Vivanco, Heidi Ullrich et moi-même, Devan Reed. Je vais gérer l'appel.

Avant de commencer, je souhaite vous rappeler à tous de bien donner votre nom avant de prendre la parole pour la transcription et l'interprétation et d'éteindre vos micros lorsque vous ne parlez pas pour éviter toute interférence.

Merci beaucoup et Bram, je vous passe la parole.

BRAM FUDZULANI : Merci beaucoup Devan. Encore une fois, bienvenue à tous au nom de moi-même, de ceux qui sont présents aujourd'hui, des dirigeants d'AFRALO.

Donc le sujet d'aujourd'hui avait fait l'objet d'un vote par les membres de la communauté pour nous préparer à la réunion de l'ICANN 72 et en particulier à la rédaction de la déclaration conjointe.

Donc je remercie d'avance nos intervenants, dont Yazid, qui va nous présenter ce sujet très important, ainsi que Paul. Et je souhaite que vous vous sentiez libre pour les questions/réponses. S'il y a des choses qui ne sont pas claires n'hésitez pas.

Je vais d'abord donner la parole aux intervenants et ensuite nous ferons donc les questions/réponses à la fin de leur présentation. Merci beaucoup.

YAZID AKANHO : Merci beaucoup Bram. Donc encore une fois c'est un plaisir pour moi d'être avec vous. Je suis là avec ma famille AFRALO. Et Paul est également présent, il va présenter avec moi. Il est spécialiste de la relation avec la partie prenante africaine. Donc nous travaillons tous les deux dans cette région de l'Afrique et du Moyen-Orient.

Alors, excusez-moi, je n'ai pas l'option de partager mon écran, est-ce que je pourrais l'avoir ?

DEVAN REED : Oui, tout à fait, un petit instant.

YAZID AKANHO : Et je pense que Paul devrait également être co-hôte.

DEVAN REED : Oui, tout à fait.

YAZID AKANHO : J'espère que vous voyez la diapositive. Très bien, merci.

Donc, aujourd'hui, nous allons parler de manière très large du sujet de la sécurité des données. Et nous mettrons l'accent sur la sécurité des données du DNS. Donc le sujet est très vaste. Et même les données du DNS, en soi, c'est un sujet très vaste. On pourrait y passer toute une journée. Mais nous allons essayer de vous donner les éléments les plus importants relatifs à la sécurité des données du DNS au cours des 30 minutes à venir.

Et donc nous espérons que, grâce à vos questions, grâce à vos commentaires, et bien cette session sera intéressante.

Donc l'ordre du jour est relativement simple, nous allons vous donner un aperçu global du DNS, pour ceux qui participent je vous rappelle que nous avons organisé une séance sur le DNS la dernière fois. Ensuite, nous présenterons la sécurité des données du DNS, nous considèrerons l'architecture globale du DNS. Ensuite nous passerons aux aspects plus spécifiques de la sécurité des données du DNS, dont le DNSSEC, la protection de la vie privée, l'IDRP ainsi que différentes initiatives de l'ICANN qui appuient cet écosystème.

Alors, commençons par le DNS. Assez rapidement. Pour ceux qui ont déjà participé à la séance précédente sur le renforcement des capacités sur le DNS, nous avons déjà expliqué qu'il s'agit d'un annuaire pour internet. C'est le lieu où nous essayons de faire correspondre les adresses IP et les dispositifs, mais il faut donc relier une adresse IP au dispositif de manière à être connecté et à être identifié sur internet.

Donc aujourd'hui, internet est composé de plus de 100 milles réseaux, il s'agit de milliards de dispositifs qui sont connectés.

Et donc, sachant que l'internet a augmenté en termes de nombre de dispositifs et de services qui sont connectés, nous avons également observé le besoin d'avoir ou de mettre en place une meilleure organisation, un meilleur système, pour traduire ces adresses IP en email et les emails en adresse IP.

Donc voilà comment ceci a été inventé en 1993. Donc il y avait John Postel qui a participé à cette invention. Donc c'est une sorte de hiérarchie avec des points d'entrée, la racine. La racine est gérée par l'ICANN.

Au-delà de la racine nous avons ce que l'on appelle le domaine de premier niveau, le deuxième niveau et le troisième niveau.

Lorsque l'on regarde les dispositifs et comment la résolution se fait – parce qu'encore une fois en tant qu'être humain tout ce que nous faisons c'est de taper les noms, mais le dispositif doit charger l'adresse IP qui correspond au nom qui est tapé dans le navigateur par exemple – donc le dispositif parle au résolveur minimum, il s'agit d'un logiciel qui est intégré dans le système d'exploitation, mais ce résolveur minimum ne connait probablement pas cette adresse IP. Donc ce résolveur minimum va envoyer une requête à un serveur externe qu'on appelle le serveur récursif. Et donc ce serveur récursif se trouve dans un réseau local. Et donc le rôle de ce résolveur récursif est en fait d'envoyer une requête à différents serveurs qui font autorité et qui sont les lieux où le lien est effectué entre les noms et les adresses IP. Donc ces serveurs de nom faisant autorité renvoient leur réponse sur la base de la

configuration qu'ils ont. Une fois que le serveur récursif a posé sa question au serveur faisant autorité et qu'il reçoit l'adresse dont a besoin l'utilisateur, il peut l'envoyer à l'utilisateur.

Donc ce n'est qu'une fois que ce processus de résolution aura été effectué que l'utilisateur pourra rentrer dans le site web. Il y aura donc une requête http à ce site web pour obtenir le site.

Donc vous voyez là un exemple d'un utilisateur qui utilise son téléphone iPhone pour aller sur ICANN.ORG.

Donc, encore une fois, si ce processus de résolution de DNS échoue, l'utilisateur ne pourra jamais avoir accès au site web qu'il demande.

Alors, il y a d'autres problèmes qui peuvent se produire et donc nous allons essayer de les expliquer avec les diapositives suivantes.

Parlons maintenant de la sécurité des données. En termes de sécurité, il y a 3 grandes fonctionnalités, 3 grandes fonctions ou 3 grands objectifs en fait.

Premièrement la confidentialité. Qu'est-ce qu'on veut dire par là ? L'objectif est d'éviter tout accès ou toute utilisation non autorisée d'information ou de données.

Deuxièmement, l'intégrité : comment nous assurons-nous que les informations ne sont pas modifiées par quel qu'entité que ce soit.

Et, dernière chose, l'authenticité et la disponibilité : comment s'assurer que les données sont disponibles à ceux qui y ont droit ? Donc de manière fiable.

Le DNS a été victime, au fil des années, d'un certain nombre d'attaques parce que le DNS, en tant qu'infrastructure, est un point important, une infrastructure importante de l'internet. Donc au fil des années nous avons pu observer plusieurs attaques qui avaient pour objectif de modifier les données du DNS pour rendre le DNS non disponible. Les attaques DDOS, certaines attaques de piratages pour modifier les données du DNS qui se trouvent dans le cache. Nous avons pu également observer des attaques de l'homme du milieu et d'autres types d'attaques : empoisonnement de cache, redirection, etc.

Donc au fil des années, nous avons essayé de voir quels étaient les points ciblés, ou potentiellement ciblés, parce que sans ces informations il n'est pas possible de fournir de mécanismes de protection à cette infrastructure du DNS.

Donc si on regarde l'infrastructure actuelle sur la diapositive, l'utilisateur est considéré être derrière le résolveur minimum à gauche. Ce résolveur minimum parle avec le récursif et il peut y avoir une attaque de l'homme du milieu à ce niveau. Donc il y a des personnes qui n'ont pas l'autorisation et qui pourraient avoir un phénomène d'empoisonnement du cache. Donc entre les résolveurs récursifs et celui faisant autorité il peut y avoir cette attaque de l'homme du milieu.

Et, lorsque vous êtes avec les serveurs faisant autorité, vous avez les données qui peuvent être corrompues à ce niveau, et ce pour les adresses de protocole internet. Il y a donc des pirates qui peuvent essayer de corrompre ces données. Et il y a différentes manières pour corrompre ces données.

Et ces données, d'où proviennent-elles ? Elles proviennent des titulaires de nom de domaine qui passent par les bureaux d'enregistrement et qui essayent donc de s'inscrire pour des noms de domaine. Donc nous avons vu différents types d'attaques.

Maintenant, voyons un petit peu comment on peut mieux comprendre la sécurisation de l'infrastructure du DNS. Il y a diverses techniques et méthodes que nous pouvons utiliser, par exemple pour la protection des serveurs récursifs nous pouvons déployer des contrôles d'accès, il y a différents niveaux, il y a différents vétos, différents mécanismes qui existent pour la protection des serveurs récursifs. En ce qui concerne les serveurs faisant autorité, il y a également beaucoup de mécanismes qui existent pour s'assurer qu'il y a une forte sécurité et une bonne disponibilité des données.

Lorsque l'on parle de la protection des données du DNS, comment protéger ces données ? Vous connaissez déjà sûrement ce terme de DNSSEC, nous allons revenir un petit peu là-dessus, et également les données passent des serveurs faisant autorité à d'autres serveurs, donc comment peut-on s'assurer que l'on protège ces transactions du DNS qui sont faits entre les serveurs principaux et secondaires ?

Il y a deux techniques principales. La première, bien connue, TC, le protocole de signature de transaction. Ça, ça a été publié par l'IETF il y a seulement quelques jours. Il y a également le transfert de zone complet sur TLF. Donc ça vous pouvez regarder le document RFC 9103 qui vient de sortir. Tout nouveau et tout à fait intéressant. Et il y a les requêtes des fichiers de zone en utilisant le DNS. Il y a également bien entendu,

pour le respect de la vie privée, il y a le DoT, [DsurT] et DoH sur lequel nous allons également revenir.

Donc nous avons cette architecture du DNS. Essayons de bien placer les techniques que nous allons utiliser au bon endroit.

On a parlé déjà des verrouillages qui peuvent être effectués des registres. Ça c'est un mécanisme qui permet d'assurer que les titulaires de nom de domaine autorisent bien les modifications des données. Nous avons également les requêtes DoT entre les serveurs primaires et secondaires. Nous avons également le DoH et plusieurs techniques qui, en fait, peuvent être utilisées par les titulaires de nom de domaine.

Nous allons voir, étape par étape, quels sont ces mécanismes du DNS pour la protection contre les attaques [SNTP] du protocole simple de transfert de courrier. Certaines sont tout simplement basées sur le DNS. Donc dans les logiciels il y a possibilité de sécuriser les courriels, principalement, la sécurité des emails. Lorsque l'on a un nom de domaine, on peut définir 3 types de fichiers DNS pour la sécurité, c'est un protocole simple de transfert du courrier. Le premier c'est le cadre de politique d'envoi, donc ça c'est identifier les emails et il y a des rapports qui sont effectués. On enregistre donc… Je ne vais pas rentrer dans les détails techniques, c'est assez complexe, mais je voulais parler un peu de ces protocoles qui permettent de sécuriser les courriels et l'infrastructure des emails en définissant, par exemple, les serveurs autorisés pour envoyer des emails.

En ce qui concerne les systèmes, la gestion des systèmes, on a parlé des serveurs principaux, secondaires, on a parlé des systèmes d'enregistrement, on a parlé des aspects matériels, mais nous devons

nous assurer que tous les systèmes de protection sont bien appliqués. Et tout cela doit être revu régulièrement. Qui accède à ces systèmes ? L'authentification est extrêmement importante, les mots de passe sont extrêmement importants. On parlera un peu plus tard du DNSSEC également.

Pour ceux qui ne connaissent pas encore bien le DNSSEC, ces extensions de sécurité pour le système des noms de domaine, DNSSEC, permettent de sécuriser le DNS. C'est un protocole en fait qui rajoute de la sécurité au niveau du DNS. Ça, ça existe depuis 2005 à peu près. Donc nous avons des standards du DNSSEC qui ont été publiés dans RFC 4033/4034/4035. Vous pouvez vous référer à cela sur le DNSSEC.

Donc depuis 2005 nous utilisons le DNSSEC, les extensions de sécurité, et la racine de l'internet a été sécurité en 2018. Au niveau technique, nous avons fait le roulement de la clef, de la cryptographie, donc de ces clefs pour la sécurité du DNS. Il y a donc toute une cryptographie qui est utilisée, cryptographie à clef publique pour sécuriser les données, il y a une signature des données.

Cela assure l'authenticité de ces données du DNS et les titulaires de nom de domaine qui veulent sécuriser leur fichier de zone, leur domaine, doivent signer les données DNS.

Mais, d'un autre côté, il y a une autre opération qui se déroule et qui est requise de la part des opérateurs du DNS, des prestataires de service internet, qui doivent faire la validation du DNSSEC. Parce que d'un côté nous devons signer les domaines, mais d'un autre côté nous devons valider ces domaines. Donc avec les serveurs récursifs nous avons une

validation DNSSEC. Et cela permet donc qu'il y ait moins d'attaques et qu'il n'y ait pas d'abus ou d'utilisation malveillante.

Que fait ou non le DNSSEC ? Nous avons cette cryptographie à clef publique, nous avons cette signature numérique qui fournissent une authenticité sur l'origine des données. Cela nous assure que les données sont intègres solides, qu'il n'y a pas eu de modification par qui que soit du serveur de nom à l'utilisateur. Donc cela protège contre l'usurpation des données du DNS mais ne fournit pas une confidentialité des données. Il n'y a pas de chiffrement.

Donc il y a une chaine de confiance qui existe au niveau du DNSSEC, nous avons une validation à partir de la racine, une validation des fichiers et des données. Selon où vous trouvez dans la hiérarchie du DNS vous avez cette chaine de confiance. Et, à un niveau technique, il y a des configurations qui existent et il y a diverses informations sur les différents « parents » et c'est la manière dont cela fonctionne, cette chaine de confiance avec la signature des données.

Donc vous avez également des recommandations, si vous avez des entreprises vous devez signer vos noms de domaine d'entreprise, vous devez permettre la validation du DNSSEC, par exemple, c'est très important.

Pour ceux qui sont intéressés par les statistiques, je vais aller rapidement, elles sont à l'écran. Aujourd'hui tous les gTLD sont signés par rapport au DNSSEC, mais au niveau des ccTLD, nous avons encore du travail à faire et notamment en Afrique. Nous n'avons que 21 % des ccTLD en Afrique qui ont signé avec le DNSSEC. Et lorsqu'on parle de

validation du DNSSEC avec les résolveurs, on est à 34 % globalement et 28 % au niveau de l'Afrique.

Donc nous avons encore beaucoup de travail à effectuer. Et la communauté des utilisateurs finaux, des internautes, joue un rôle important, est un partenaire pour atteindre ces niveaux.

Nous allons maintenant faire un petit sondage, à partir de cette présentation. Et je vais donc demander au personnel de me soutenir pour cela.

Nous allons lancer le sondage et ensuite je passerai la parole à mon collègue Paul Muchène. Paul je vous passe la parole et le staff lance le premier sondage….

Ha, désolé, je crois qu'il y a une petite erreur, on va passer au deuxième sondage, je crois qu'on a oublié de faire le premier sondage, on va passer au deuxième sondage. Désolé pour cela. Nous allons parler des techniques de chiffrement du DNS. Donc, quelles sont les techniques que vous connaissez pour chiffrer le DNS ? A, DoB et D/C, D/T et D/V, C : D/H et D/T, aucune de ces réponses en quatrième point. Vous pouvez répondre au sondage.

Donc on va vous donner quelques secondes pour remplir le questionnaire. 10 secondes.

DEVAN REED : Nous avons 20 réponses maintenant sur 43. Je ne sais pas si vous souhaitez attendre un petit peu…

PAUL MUCHENE : On pourrait peut-être lire les réponses ?

DEVAN REED : Très bien. Donc voilà les réponses. Donc voilà la réponse : 55 % ont dit aucune réponse, 35 % disent DoH et DoT, 10 % disent DoT et DOB. Et la bonne réponse c'est DoH et DoT.

PAUL MUCHENE : Je vais justement en parler pendant le reste de la présentation. Donc Yazid, si vous pouvez afficher la diapo suivante ? Merci.

Donc Yazid vous a parlé de deux aspects de la sécurité des données du DNS, il a parlé surtout de l'intégrité des données et de ce que fait le DNSSEC pour renforcer l'intégrité. Il a également parlé des techniques, par exemple la redondance ou NCAP.

Donc moi je vais m'attaquer à la question de la confidentialité. Yazid a déjà mentionné – et j'ai le même sentiment – que le DNS à la base, n'avait pas été conçu avec la question de la sécurité prise en considération. Donc au fil des années, ce qu'on a pu observer – donc de 83 à maintenant – c'est que la sécurité a dû être améliorée avec le temps. Donc il y a également la confidentialité qui a été mise en œuvre dans le DNS, assez récemment, et donc je vais parler des deux technologies qui sont prééminentes et qui ont été utilisées dans le DNS pour protéger les données parties tierces qui souhaiteraient écouter ou interférer.

Donc, du point de vue de l'ICANN, il nous semble que la protection de la vie privée est très importante pour l'utilisateur. Et donc le DNSSEC

protège les réponses entre résolveurs des attaques, celles de l'homme du milieu et autres qui, parfois, injectent de mauvaises requêtes, de fausses requêtes et qui affectent le résolveur ou l'utilisateur final.

Mais le chiffrement implique certaines politiques techniques. Nous n'allons pas parler de tout ceci, nous n'avons pas le temps, mais si la communauté AFRALO est intéressée on pourrait consacrer un webinaire à parler de la protection de la vie privée sur le DNS. Mais pour l'instant, nous allons parler du DoT et du DoH, donc DNS sur [inaudible] et DNS sur https.

Donc la première chose que je dois vous dire c'est que le chiffrement est un des moyens que nous avons, donc c'est là-dessus que nous allons baser notre discussion.

Prochaine diapositive Yazid.

Donc il existe actuellement deux protocoles standardisés, donc DNS/TLS et DNS sur https. Donc il y a deux documents qui en parlent : le RFC7858 et RFC8484.

Donc ceci est similaire du point de vue de la sécurité. Dans ces deux premiers documents sur le DoT, 7858 et 8094, et la deuxième option, DoH, c'est RFC84, mais il y a eu une certaine controverse par rapport à ceci. Ce qui n'est pas standardisé mais qui a été utilisé dans le cadre de beaucoup de mises en œuvre, c'est le DNSScrypt. Donc il y a beaucoup de chevauchement entre ces deux technologies. Mais une des différences principales est que le DNS/HTTPS se mélange avec les requêtes. Donc ce qu'il se passe c'est que vous envoyez des requêtes

chiffrées entre dispositifs et il y a un résolveur qui a un canal chiffré avec 443, mais dans le DoT, le canal chiffré est de CCP853

[L'interprète s'excuse nous avons un problème de son avec Paul]

Alors ces technologies permettent d'éviter l'intervention de parties tierces, mais notre point de vue à l'ICANN, à la base, c'est que filtrer peut être bénéfique. Alors, nous ne parlons pas de censure, mais nous parlons de pratiques malicieuses, de spam, de programmes malveillants. Et donc il faut bien distinguer et discriminer le trafic, celui qui peut nuire à l'utilisateur final, et le reste.

Pour nous la protection de la vie privée est très importante pour l'utilisateur final et nous essayons de promouvoir la protection de la vie privée. Par ailleurs, nous croyons que le DNS doit être protégé, même si le DoT et le DoH fournissent la confidentialité nous pensons qu'en termes d'intégrité de données, il faut qu'il y ait protection…

[L'interprète s'excuse encore une fois, le son n'est pas très bon]

Donc il y a certaines décisions de networking qui doivent être prises et donc, avec des technologies telles que le Dot et le Doh, il faut prendre ceci en compte.

Pour une description complète de notre prise de position et des caractéristiques du DoT et du Doh, vous pouvez aller voir le document OCTO 003 qui parle des implications du DNS chiffré.

Diapo suivante.

Donc, actuellement, en ce qui concerne la mise en œuvre du DNS sur HTTPS, Mozzilla travaille en partenaire avec CloudFair et il y a une option

dans le navigateur Firefox qui permet d'activer le DoH, de manière à pouvoir signer les requêtes. Et Google, dans le cadre de leur service Public DNS 8.8.8.8 travaille avec le DoH également. Donc voilà où nous en sommes en termes de DoH.

Mais par rapport à la zone racine, il faut savoir que les opérateurs de serveur racine ne sont pas à l'aise pour adopter ce chiffrement du DNS, ils ont certaines préoccupations par rapport à ce chiffrement.

Et donc, étant donné le rôle critique de ces serveurs de nom, ils sont souvent cibles d'attaques [inaudible]

Donc vous avez le lien ici de leur déclaration, de ces opérateurs de serveurs racine, vous pouvez y avoir accès.

Par contre, plutôt que le DNS sur le HTTPS et plutôt que le chiffrement du DNS, les opérateurs de service utilisent la minimisation QName et le cache DNSSEC aggressif. Donc voilà ce qu'ils utilisent. Donc la minimisation QName est une autre manière de protéger la vie privée et de minimiser l'exposition aux requêtes. Donc là vous envoyez aussi peu d'informations que possible vers le serveur faisant autorité. Et donc nous sommes en train d'essayer de les aider de les aider pour essayer de les aider pour améliorer la protection de la vie privée. Vous avez le RFC 78 qui vous explique le fonctionnement.

Nous avons également la solution du cache agressif de DNSSEC. Et donc dans cette fonctionnalité on utilise le [NEXTSEC], prochaine sécurité. Et cette technique cache uniquement les noms de domaine qui existent dans… C'est basé sur les noms qui existent dans la racine et ceux qui n'existent pas.

Donc la dernière partie de ma présentation c'est sur le protocole d'accès aux données d'enregistrement, le RDAP.

Le RDAP est un protocole qui a été conçu par le groupe de travail de génie internet, l'IETF, et c'est un protocole très intéressant parce qu'il est défini par les RFC 7480 à 93, donc un certain nombre d'entre eux.

Alors le WHOIS a été utilisé depuis le tout de début de l'internet et nous sommes en train de travailler à son remplacement. Il est basé sur des blocs d'adresses IP et les systèmes autonomes.

Alors, on va revenir à la diapositive précédente.

Donc à l'inverse du WHOIS… Le WHOIS permet l'accès à différentes informations, les gens sont de plus en plus conscients de leurs droits d'accès et donc le RDAP, à l'inverse du WHOIS, peut être utilisé dans différentes langues et dans différents scripts. Donc il y a différentes options.

Par ailleurs le RDAP, lorsqu'il est mis en œuvre, est un protocole beaucoup plus robuste et plus sécurisé car il utilise le HTTPS qui, en fait, fournit un chiffrement entre les serveurs. Et, en même temps, le WHOIS n'avait pas de format d'attente et donc cela est beaucoup plus simple.

Alors, une des choses positives par rapport au RDAP, surtout pour les développeurs, c'est que le protocole RDAP est écrit en [Json] donc on peut utiliser une langue telle que le Json… Excusez-moi pour cette interruption, une alerte en anglais.

Donc voilà certaines des différences entre le WHOIS et le RDAP.Donc voilà quelques informations.

Donc il y a des initiatives de l'ICANN pour soutenir un écosystème sécurisé du DNS. Les initiatives sur lesquelles travaille l'ICANN.

Il y a donc un partage de connaissances et des normes pour la sécurité des noms de domaine, [inaudible] DNS pour améliorer la sécurité et la résilience du DNS. Il y a des projets en ce moment qui sont faits à l'ICANN, avec ISOC notamment. Et au niveau de l'ICANN nous travaillons à cela puisque nous avons un rôle opérationnel dans le DNS.

Il y a donc le système DAAR de signalement des cas d'utilisation malveillante des noms de domaine. Au Kenya, en Tanzanie et en Malawi nous faisons beaucoup au niveau du DAAR et nous voulons travailler avec plus de ccTLD pour travailler au rapport de signalement DAAR. Nous avons ensuite le DNS Sticker, le signalement et la collecte d'information sur des menaces à la sécurité des domaines, pour identifier en rapport avec la pandémie de Covid les utilisations malveillantes du DNS qui ont été effectuées pour profiter de cette pandémie. Nous avons des collègues à OCTO qui travaillent beaucoup à cela. Nous avons également des indicateurs de santé des technologies et identificateurs, ITHI. Et ces identificateurs de santé et technologie fonctionnent, ainsi que l'initiative de facilitation de la sécurité du système des noms de domaine, DFFI qui est géré par Goran Marby, par notre PDG à l'ICANN, avec des experts de la sécurité dans la communauté. C'est une initiative pour identifier au niveau de tout le DNS les problèmes de sécurité. Nous avons des nouvelles stratégies, notamment une stratégie sur le serveur racine qui est gérée par l'ICANN, IMRS. Et nous avons également au niveau de l'engagement technique des programmes pour renforcer les capacités, des programmes de

formation pour les internautes, pour les opérateurs également, pour vraiment faire le maximum pour la sécurité du DNS.

Et donc nous avons des ressources supplémentaires que je vous indique à l'écran. Vous pouvez cliquer sur ces liens, vous avez des catalogues.

Passons à la dernière diapo.

Merci beaucoup de votre attention, je vais donc maintenant être prêt à répondre à vos questions.

BRAM FUDZULANI : Je crois qu'il y a une main qui était levée un petit peu plus tôt. Abdulkarim, vous aviez levé la main, je crois. Est-ce qu'on a déjà répondu à la question que vous aviez ? Très bien. Donc je vais vous inviter à poser vos questions. Je sais qu'il y a des questions dans le chat également, mais je crois qu'on a répondu à la plupart des questions dans le chat. Mais si quelqu'un veut prendre la parole et poser une question à nos présentateurs, vous pouvez l'effectuer maintenant.

[L'interprète s'excuse, nous entendons très mal Bram, il y a des interférences et des coupures actuellement]

Très bien. Donc allez-y. Enoch, allez-y, vous pouvez parler.

Nous n'entendons pas Enoch. Enoch, si vous parlez, on ne vous entend pas, on ne peut absolument pas entendre votre question, nous n'avez pas du tout de volume. Enoch, on n'entend pas votre voix. Désolé, on ne vous entend pas.

CLAUDIA RUIZ : Nous avons également une question dans le chat, c'est une question en français. Nous avons deux questions, une d'Olivier et une autre de Gabriel Bombambo.

BRAM FUDZULANI : Oui, lisez la question s'il vous plait.

CLAUDIA RUIZ : Je vais lire la question d'Olivier : quand est-ce que RDAP va totalement remplacer WHOIS ?

NON IDENTIFIÉ : Ce qu'il s'est passé c'est que nous avons recherché une alternative à WHOIS et il y a des registres, tout particulièrement au niveau des gTLD où il y a des obligations contractuelles, qui doivent mettre en œuvre RDAP. Et pour la plupart des gTLD, ils sont en train d'utiliser RDAP de plus en plus. Ça va prendre un petit peu de temps pour les ccTLD notamment, les politiques sont différentes et il y a des services de requête qui sont un petit peu différents pour les ccTLD. Et, je ne veux pas donner un calendrier très précis, mais je pense que ça va être assez graduel et on va le voir de plus en plus, l'utilisation du RDAP, à l'avenir.

YAZID AKANHO: Je vais répondre à la deuxième question, elle était en français, est—ce que vous voulez que je réponde en français ou en anglais ?

CLAUDIA RUIZ : Lisez la question en anglais pour qu'on puisse l'interpréter en français.

YAZID AKANHO: La question était : est-ce que le seul chiffrement utilisé est asymétrique dans la sécurité du DNS, demandait Gabriel Bombambo et je vais clarifier cela.

Gabriel, vous devez parler du DNSSEC et j'aimerais vous rappeler que le DNSSEC est juste une signature des données, ce n'est pas un chiffrement, les données du DNSSEC ne sont pas chiffrées. Et nous avons besoin d'asymétrie, en effet, pour la signature des données, on a des protocoles asymétriques de signature des données dans le cadre d'une clef cryptographique qui est utilisée dans le cadre du DNSSEC. Et en ce qui concerne le respect de la vie privée, là, vous avez un système de données chiffrées entre les résolveurs récursifs et [inaudible], on a le HTTPS et le TLS.

J'espère que cela a répondu à votre question.

BRAM FUDZULANI : Une question de Edmond, Edmond Kungwalo, vous avez la main.

EDMOND KUNGWALO: Oui, je voudrais mieux comprendre l'avenir du DNS, le respect de la vie privée des utilisateurs. Pensez-vous que les règles doivent utiliser le trafic des utilisateurs ? Est-ce que ça ce n'est pas un problème de respect de la vie privée de regarder de près le trafic des utilisateurs ?

PAUL MUCHENE: Je vais essayer de répondre à cela. Oui, un des problèmes avec le DoH et le DoT d'ailleurs c'est que cela rend plus difficile pour un opérateur de conduire un travail sur les différents trafics. Donc un attaquant pourrait donc utiliser cela et essayer de prendre le contrôle. Et ça c'est un problème en fait. Il y a un document de OCTO qui parle de cela, de l'utilisation de certaines de ces technologies et le respect de la vie privée des utilisateurs. Ça, ça crée des problèmes pour les opérateurs. Donc plus de vie privée pour les utilisateurs finaux veut souvent dire des questions technologiques qui se posent pour les opérateurs.

J'espère avoir répondu à votre question.

EDMOND KUNGWALO : Oui merci.

BRAM FUDZULANI : Il y a une main qui était levée ou qui a été baissée, je ne sais pas si la question a été couverte. Lawrence ?

LAWRENCE OLAWALE-ROBERT: Par rapport au DNSSEC, par rapport aux données présentées et l'adoption par les ccTLD, ma question était sur les problèmes éventuels pour cette adoption. Il y a un niveau technique pour maintenir les fichiers de zone, je pense que c'est exact.

YAZID AKANHO: Merci Lawrence. Oui, comme dans tout autre mécanisme de sécurité et d'infrastructure de sécurité, il y a une nouvelle expérience et de

nouvelles compétences et qualifications à acquérir pour maintenir au quotidien les nouveaux systèmes. Et le DNSSEC est comme cela, c'est pareil. Le DNSSEC, en fait, utilise des clefs, des clefs publiques et une cryptographie. Il faut générer ces clefs cryptographiques, il faut signer les zones, il faut que la signature n'expire pas avant de générer de nouvelles caractéristiques et ainsi de suite. Donc oui, c'est des défis techniques à relever et c'est pour cela que l'équipe d'engagement technique de l'ICANN est de plus en plus renforcée, pour donner plus de formation pratique à la communauté, qu'elle soit la communauté technique ou la communauté des gouvernements, des internautes, pour fournir des compétences de connaissances de l'infrastructure. Donc il y a des mécanismes à connaitre. Mais des possibilités également de se former à ces connaissances.

BRAM FUDZULANI : Merci beaucoup. Donc vous pouvez envoyer également dans le chat si vous n'êtes pas en mesure de prendre la parole. Enoch nous parle donc de ce qui est utilisé par les gouvernements, par les cybercriminels pour accéder des données chiffrées sans la connaissance de la personne qui envoie ou qui reçoit. Donc est-ce que le DNSSEC est donc vulnérable à ces menaces par rapport aux autorités sécuritaires ? Qu'en est-il ? Paul ?

PAUL MUCHENE: Le DNSSEC a des protocoles de sécurité qui ne sont pas gérés, notamment la confidentialité comme on l'a vu. Donc pour ce qui est des gouvernements, des autorités qui voudraient avoir accès à ces données, les forces de sécurités par exemple de certains gouvernements, le gouvernement en question est en mesure d'avoir accès à ces données,

parce qu'elles ne sont pas protégées par le DNSSEC qui ne gère pas la confidentialité des données. Vous devez utiliser d'autres technologies comme le DoT.

Mais cela dépend de la mise en œuvre lors de la signature de la zone. Donc il y a différents algorithmes qui existent et qui peuvent être mis en place. Mais il y a des opérateurs qui, même lorsque c'est standardisé puisque le DNSSEC existe depuis 2005, n'ont toujours pas l'utilisation du DNSSEC qui est assurée.

Donc il y a eu des problèmes à ce niveau. En 2004, il y a eu des problèmes au niveau des algorithmes. Vous êtes vulnérable. Cela dépend des clefs qui sont utilisées pour signer les zones. Donc ce qui est recommandé maintenant est d'utiliser d'autres algorithmes et vous avez des informations plus précises là-dessus, vous avez tout un système de cryptographie qui existe et les opérateurs de zone, y compris les ccTLD, doivent utiliser les algorithmes 13 par exemple, qui fournissent beaucoup plus de sécurité. Ensuite, le DNSSEC ne gère pas la confidentialité des données, comme nous l'avons vu. Nous avons par exemple une entité qui peut faire des requêtes et connaitre donc vos envois. Donc l'accès des cybercriminels, c'est là où le DNSSEC protège beaucoup plus.

Je vais vous donner un exemple. Donc s'il y a quelqu'un qui souhaite pirater une zone ou alors un deuxième niveau pour l'opérateur [RSO] en fait il y a manipulation. Partons du principe, par exemple, que l'opérateur de zone a fait sa diligence raisonnable par rapport au DNSSEC mais le cyberattaquant a accès au serveur. Donc ce qu'il se passe c'est que le cyberattaquant, ce qu'il se passe c'est que lorsque

quelqu'un par exemple envoie une requête à la zone, par exemple la zone BANQUE.COM qui a une adresse IP légitime, mais étant donné que BANQUE.COM a été signé, le résolveur pourra vérifier la signature de BANQUE.COM, il pourra vérifier la signature avant et il vérifiera qu'elle correspond au moment de la signature et ensuite il vérifiera les données qui ont été modifiées et il y aura comparaison des résultats.

[Excusez-nous, une petite interruption sur la ligne anglaise].

TIJANI BEN JEMAA : Est-ce que je peux vous interrompre un instant ? Nous avons déjà dépassé les 60 minutes de 5 minutes, donc on peut effectivement continuer quelques minutes et répondre aux questions qui arrivent si c'est possible. Voilà, je voulais juste faire cette petite annonce. Je vous repasse la parole, Paul.

PAUL MUCHENE: Merci Tijani. Donc à la base, ce qu'il se passe c'est que la validation de DNS vérifie que l'attaquant a modifié les données et donc toutes les requêtes à BANQUE.COM seront rejetées, il y aura un message d'erreur. Ceci permet d'éviter que la personne redirige ses informations vers une infrastructure du pirate. Donc le DNSSEC permet d'éviter toute une [inaudible] des données de DNS. J'espère que ceci répond à votre question.

BRAM FUDZULANI : Voilà, donc je pense que nous allons bientôt conclure. Je crois que la plupart de questions envoyées par chat ont reçu une réponse. Sauf s'il y

a des questions spécifiques de dernière minute… Ou une question de suivi, des personnes qui, peut-être, souhaitent envoyer une dernière question… S'il n'y a pas d'autres questions, et bien je vais repasser la parole à Tijani pour qu'il puisse avoir le dernier mot. Allez-y Tijani, vous avez la parole.

TIJANI BEN JEMAA : Merci beaucoup Bram et merci à nos deux excellents intervenants. Je suis très fier de ces jeunes africains qui ont rejoint l'ICANN en particulier dans le domaine technique. C'est vraiment très utile parce qu'ils ont vraiment d'excellentes connaissances précises de haut niveau et puis ils ont beaucoup d'énergie et nous en avons besoin à l'ICANN.

Donc merci beaucoup, nous sommes très fiers de vous et nous vous remercions vraiment de vous êtes rendu disponibles. À chaque fois que nous vous le demandons vous l'êtes. J'ai demandé à Yazid de faire cette présentation et Paul s'est porté volontaire, je souhaite réellement le remercier parce que c'est lui qui s'est proposé. Donc je vous remercie tous les deux. Je crois que c'était très utile pour la communauté.

Et je dois vous dire qu'il nous reste 1 webinaire pour le mois de novembre, qui sera le dernier de cette année. J'espère que nous pourrons l'organiser. Nous avons beaucoup de choses à faire au mois de novembre, mais nous allons quand même essayer de l'avoir.

Je remercie le personnel, les interprètes et vous tous qui êtes là. Merci d'avoir contribué à la préparation de la rédaction de cette déclaration et participé à la rédaction de la déclaration, c'est le seul moyen pour

apprendre, pour acquérir des connaissances et aussi pour exprimer le point de vue de l'Afrique.

Merci à tous, ce webinaire est désormais terminé. Merci.

DEVAN REED : Merci à tous, nous vous souhaitons une excellente journée.

[FIN DE LA TRANSCRIPTION]