ICANN72 | Semaine de préparation – Présentation de l'initiative de facilitation de la sécurité du DNS - groupe d'étude technique (DSFI-TSG)
Jeudi 14 octobre 2021 – 13h00 à 14h00 PDT

WENDY PROFIT : On va lancer l'enregistrement.

Bonjour et bonsoir. Bienvenue à la séance sur la présentation du groupe d'analyse technique pour l'initiative de facilitation de la sécurité dans le DNS. Je suis Wendy Profit, je suis en charge de la participation à distance pour cette séance.

Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendu à l'ICANN.

Les questions et les commentaires soumis dans le chat ne seront lus à haute voix que s'ils sont soumis dans la fenêtre de questions et réponses. Je les lirai à haute voix pendant le temps alloué par le président ou le modérateur de cette séance.

Le service d'interprétation simultanée sera disponible dans les langues des Nations Unies. Veuillez cliquer sur l'icône d'interprétation sur Zoom et sélectionnez la langue dans laquelle vous souhaitez écouter la séance.

Si vous souhaitez prendre la parole, veuillez lever la main dans la salle Zoom et lorsque le modérateur de la séance dira votre nom, notre équipe technique vous permettra d'activer votre micro. Avant de

prendre la parole, assurez-vous d'avoir sélectionné la langue dans laquelle vous allez parler dans le menu d'interprétation. Veuillez indiquer votre nom pour l'enregistrement et la langue dans laquelle vous allez parler si ce n'est pas l'anglais. Au moment de parler, veuillez mettre en sourdine tous les autres dispositifs et les notifications. Veuillez parler clairement et à un rythme raisonnable pour permettre une interprétation exacte de vos propos.

Nous vous demandons d'utiliser le menu déroulant du chat si vous souhaitez communiquer avec le travers le chat. Assurez-vous de sélectionner « Répondre à tous les panelistes et participants. » Cela permettra à tout le monde de voir votre commentaire. Veuillez noter que les discussions privées ne sont possibles qu'entre les panelistes dans le format Zoom Webinar. Tout message envoyé par un paneliste ou par un participant à un autre sera également vu par les hôtes de la séance, les co-hôtes et les autres panelistes.

Pour voir la transcription en temps réel, cliquez sur le bouton *Closed Caption* dans la barre d'outils de Zoom.

Maintenant je passe la parole à John Crain.

JOHN CRAIN : Bonjour, bon après-midi, bonne soirée à tous. En premier lieu, je vous présente les excuses de Göran Marby qui était occupé avec d'autres engagements et il m'a demandé de dire quelques mots en son nom.

Je suis John Crain, je suis le directeur de la sécurité, la stabilité et la résilience à l'ICANN du bureau du directeur de la technologie. Je

participe activement à cette initiative et comme vous le savez, la sécurité, la stabilité et la résilience du système d'identificateurs est centrale pour la mission de l'ICANN. Par conséquent, ceci est présent dans nos statuts constitutifs et dans toutes les activités que nous menons.

Göran m'a approché il y a deux ans après une série d'attaques qui s'était produites et il m'a demandé comment on pourrait améliorer la sécurité du système d'identificateurs. On a décidé de former un groupe d'experts de la communauté de l'ICANN et de personnes en dehors de l'ICANN. Vous allez savoir que Göran a reçu ce rapport de notre groupe au début de cette semaine et la semaine prochaine, il sera à votre disposition. Je tiens à remercier le groupe au nom de Göran pour son travail si ardu de manière volontaire pour travailler sur une série de recommandations depuis plus d'un an.

Personnellement, j'ai participé au groupe et j'ai été témoin de l'énorme travail qu'ils ont fait. Je les remercie énormément. Nous allons prendre toutes ces contributions en tant qu'organisation et nous allons par la suite procéder à établir comment on peut utiliser toutes ces informations afin de faciliter la sécurité du DNS.

Maintenant, je voudrais passer la parole à Merike Käo qui s'est proposée pour coordonner très gentiment tous ces efforts il y a à peu près un an et demi. Merike, je vous passe la parole.

MERIKE KÄO : Merci John.

Voici l'agenda pour la séance d'aujourd'hui. Je vais faire une présentation brève du travail fait depuis les 18 derniers mois et par la suite, je vais continuer avec les points principaux, à savoir les vecteurs d'attaque dans le système du DNS, les atténuations, les recommandations et puis nous aurons un espace pour les questions. Toutes ces sections seront présentées par un membre de notre groupe.

Comme John l'a bien dit, ce travail a été initié en mai de l'année dernière à partir d'une initiative dirigée par le PDG de l'ICANN. Il nous a demandé d'exécuter un engagement, de le matérialiser en travaillant avec la communauté sur des questions relatives à la sécurité et la stabilité.

Notre tâche avait pour fonction principale de faire des recommandations et l'ICANN devrait prendre ces recommandations pour améliorer le profit de sécurité du DNS et pour savoir s'il y avait des fonctions que l'ICANN ne devrait pas faire.

Une partie de cette initiative ou une grande partie de cette initiative a été menée à bien à cause de certaines attaques très sophistiquées qui se sont produits il y a quelques années. Nous nous sommes rendus compte à l'ICANN, tout le monde s'est rendu compte que la réponse à ces attaques sophistiquées avait été quelque chose du moment et qu'il devait y avoir une manière plus structurée de répondre à ce type d'attaques dans l'écosystème de l'internet et dans ce cas, qu'il était nécessaire de voir si l'on avait besoin d'un nouveau niveau de compréhension pour ce faire.

Dans cette diapositive, vous voyez le chronogramme de travail de notre groupe TSG. Le groupe a commencé en mai, on a formulé toute la composition du groupe et le 16 juin de l'année dernière, nous avons eu notre première réunion. La plupart du travail en été s'est concentré à répondre et à identifier certaines questions que l'on voulait aborder. Par la suite, au début de l'automne, on a commencé à avancer dans notre travail et une partie des délibérations était centrée sur les vecteurs d'attaques et les causes racines. Et on a créé une liste de priorités sur ces registres d'attaques pour identifier quels étaient les vecteurs d'attaque les plus dangereux soit disant et qui exigeaient notre attention.

Nous avons vu les mesures d'atténuation en vigueur ou qui n'étaient pas mises en place ou même celles qui manquaient. On a créé un document préliminaire qui a été terminé avec une série de recommandations. On a eu des consultations avec des experts de l'industrie. Et finalement, on a élaboré le rapport final qui a été envoyé à Göran au début de cette semaine.

Voici les membres du TSG, neuf membres, et comme vous pouvez le voir, c'est un groupe avec différents experts ayant des connaissances et des expériences différentes spécialisées en infrastructure des opérations du DNS. Ils connaissent la sécurité, les opérations des opérateurs de registre et des bien sûr, aussi les opérations de codes géographique, ils ont de l'expérience sur tout ce qui a trait aux ISP et aux réseaux de distribution de contenu. Toute cette combinaison nous a mis dans un niveau très profond.

Comme je l'ai dit tout à l'heure, nous avons mené à bien des consultations et nous avons fait une révision avec des conseillers techniques sur le document. Ils nous avaient offert des commentaires très spécifiques. Le TSG est vraiment très reconnaissant de la révision en profondeur minutieuse qui a été faite parce que cela nous a permis d'avoir un document final beaucoup plus riche quant aux recommandations.

Nous avons eu aussi le soutien de l'ICANN à différents niveaux, avec un comité de directeur DSFI TSG avec deux personnes du Conseil d'Administration de l'ICANN et deux directeurs exécutifs. Nous avons eu aussi un soutien très large d'une partie du personnel de l'ICANN, avec la gestion des programmes de communication et avec des connaissances spécifiques sur des questions déterminées, ainsi qu'un rédacteur technique principal excellent. Pour ce cas particulier, c'était une femme qui, de par ses connaissances, nous a permis d'avoir un texte très facile à lire malgré son niveau technique très profond.

Voilà ici un diagramme qui montre l'étendue et la profondeur de l'écosystème du DNS complet. On espérait que le travail prendrait un an, mais cela en fait a pris un an et demi. Cela a été fait de manière virtuelle, ce qui a présenté aussi des difficultés. Je veux remercier chacun des membres du TSG ainsi que les membres de soutien de l'ICANN parce que nous avons eu beaucoup de réunions et beaucoup d'ateliers qui prenaient deux ou trois heures, des ateliers hebdomadaires ou toutes les deux semaines, ce qui nous a permis d'arriver à ces résultats. C'était une question absolument complexe,

mais nous sommes vraiment très heureux et très fiers du travail que nous avons fait.

Maintenant, nous allons donc commencer à parler des questions de fond. Nous allons commencer par les attaques. Nous allons maintenant écouter Gavin Brown.

GAVIN BROWN : Merci Merike.

Dans cette partie de la présentation, nous allons voir les vecteurs d'attaque de l'écosystème du DNS et la technologie que nous utilisons pour faire ce travail.

Sur cette image, nous essayons de vous montrer, comme Merike l'a fait aussi, la profondeur et la portée du système qu'on a analysé du point de vue des menaces. Et nous allons voir qu'ici, on inclut ce qui a trait avec le DNS et aussi les utilisateurs et les registres. Ici, on peut voir la voie de résolution à travers les résolveurs et nous voyons aussi ce qui se passe avec les utilisateurs finaux, les titulaires de nom de domaine, les systèmes qui interagissent avec les protocoles des registres et des bureaux d'enregistrement et des personnes comme nous. Nous avons essayé de couvrir tous les systèmes de bout en bout et ceux qui étaient plus menacés.

Le processus que l'on a suivi est très semblable, d'après mon expérience, à une analyse de risques où l'on essaie d'analyser les différents vecteurs d'attaque. On a essayé de les catégoriser et d'établir les points en commun. On a vu les vecteurs d'attaques et on a

pris des expériences réelles que nous avons eues à partir de différentes attaques. Et quand nous voyons ces vecteurs, nous considérons différentes questions, par exemple quelles sont les mesures d'atténuations disponibles que l'on abordera plus en détail plus tard, savoir s'il y avait des questions ayant trait à une compréhension non suffisante du risque, savoir si le DNS était vulnérable à certaines classes d'attaques pour d'autres parties de l'écosystème du DNS.

Au niveau très général, on a établi une énorme quantité de vecteurs qui a été réduite à ce que vous voyez ici à l'écran. C'est assez vaste, mais vous verrez qu'il y en a qui sont génériques aussi, parce que les participants de l'écosystème du DNS sont des organisations et des sociétés qui ont les mêmes enjeux en termes de sécurité que toute autre organisation, une université, une banque, un opérateur de gTLD. Il y en a qui sont plus exclusifs au DNS et aussi aux protocoles et systèmes qu'ils utilisent. On pourrait donc couvrir les choix de TTL sur registres, mais aussi, on pourrait voir comment ça se passe avec le système de mots de passe par exemple. Nous verrons d'autres vecteurs tout de suite dans ces catégories.

Nous avons résumé tous ces vecteurs dans ces catégories de vecteurs d'attaques, sept catégories. On va en parler plus en détail, mais nous allons commencer avec ceux qui sont un peu plus généraux, comme la gestion des identités d'accès, un enjeu en termes de sécurité qui n'est pas exclusif à notre monde. Toute entreprise a ce genre de difficulté et tout le monde doit réfléchir à l'accès, à l'identité et aussi à ce qui est du contrôle d'accès. Mais il y a d'autres vecteurs plus spécifiques au

système du DNS, comme par exemple l'usurpation des ressources, tout ce qui a trait au déni de service et les questions ayant trait à la vulnérabilité, que ce soit au niveau des codes comme dans les protocoles. Ce sont les sélections que nous avons faites lorsque nous avons décidé de travailler sur une infrastructure déterminée, et elles peuvent faire en sorte que les systèmes soient vulnérables à ce type d'attaque. Suivante s'il vous plaît.

On commence avec le premier, la gestion des identités et des accès. Ils existent partout dans l'écosystème et dans le système d'approvisionnement. Et ils sont utilisés pour authentifier les interactions entre les participants. Si on est employé d'un registre, il faut utiliser un nom d'utilisateur et un mot de passe pour pouvoir accéder au système. Si on est un bureau d'enregistrement, il faut utiliser aussi toutes les données pour accéder au registre et la chaîne continue jusqu'à ce qu'on arrive à l'utilisateur final. Tout point de cette chaîne ou de ce système peut être compromis. En termes de sécurité, les organisations qui s'occupent d'administrer ces données doivent prendre des décisions sur la mise en œuvre de politiques qui permettent de protéger ces données pour éviter l'usurpation d'identité et la capture de ces mots de passe. On a donc travaillé dans ce domaine et on s'est focalisé sur les données des bureaux d'enregistrement, les revendeurs et aussi sur la menace d'utiliser des données compromises pour initier des transactions dans le registre où il y a l'usurpation des entités de la chaîne entre le bureau d'enregistrement et le registre. Suivante s'il vous plaît.

Nous avons ici un exemple des problèmes de contrôle d'accès et d'autorisation inadéquate. Nous voyons ici la prise de contrôle d'un sous-domaine. Nous avons ici un enregistrement dans un nom de domaine qui a un alias où l'on vise une autre ressource. Ceci permet à une attaque de prendre le contrôle de ce nom de domaine sans qu'il soit vraiment le propriétaire de ce nom de domaine.

Le prochain vecteur d'attaque concerne l'escroquerie par usurpation d'identifié de ressources. Ici, un attaquant peut faire que les requêtes de DNS soient redirigées vers un tiers. Cette redirection peut avoir plusieurs implications potentielles selon le type de système qui est usurpé ou imité. Ceci peut se produire dans le cas où cela se fait, comme une tactique commerciale légitime comme avec des portails captifs qui limitent l'accès d'un réseau interne à l'internet public. Il existe également des cas où cela entraîne une redirection vers une cible malveillante par l'installation d'un programme malveillant ou ce peut être utilisé pour collecter des données d'utilisateurs finaux par exemple. Ceci pourrait être mis en œuvre par l'usurpation de l'identité d'un résolveur récursif et de l'identité d'un serveur faisant autorité ou par l'usurpation d'identité d'infrastructure de domaines similaires, de domaines de télécopies. Nous pourrions dire que dans ce cas-là, l'objectif de ces attaques, c'est les utilisateurs de l'infrastructure et non pas les utilisateurs finaux.

Il y a aussi les certificats frauduleux et la manipulation de routage qui sont aussi utilisés comme un vecteur d'attaque. Nous avons ici un exemple de ce dont nous parlions quand nous parlions d'usurpation

d'identité de ressources. Ces attaques de domaines de télécopies, les attaques homographiques sont les exemples les plus typiques.

Le prochain vecteur d'attaque concerne les vulnérabilités de codes et de protocoles. Il y a différents problèmes ou différents défis à relever ici pour ces deux types de vulnérabilité quand il y a un problème avec le logiciel du DNS et cela est atténué de manière différente lorsque le problème se trouve au niveau du protocole. Quand il y a un problème avec le protocole du DNS, comme cela a été dit, il y a toute une série de vulnérabilité. Il y a par exemple l'attaque Kaminski. Les vulnérabilités du protocole altèrent ces protocoles et provoquent des problèmes d'interopérabilité. Il faut travailler sur ce fait en contact avec toutes les parties prenantes parce que cela pourrait déstabiliser le système. Et ces vulnérabilités doivent être abordées. Elles peuvent avoir des impacts très négatifs sur les services vulnérables. Il y a l'empoisonnement du cache par exemple. Ce serait une vulnérabilité des protocoles.

Là, vous avez un exemple de la manière dont l'empoisonnement du cache du DNS se fait. Là, vous voyez ces flèches. Lorsqu'un serveur récursif reçoit une requête d'un utilisateur final qui cherche icann.org, un attaquant peut passer cette consultation et envoyer une réponse frauduleuse au serveur récursif avant que la réponse du serveur faisant autorité n'arrive. Dans ce cas-là, la fausse réponse est envoyée à l'utilisateur final avant la réception de la réponse légitime au serveur récursif.

Quels sont les choix d'infrastructure maintenant ? Dans ces situations, ce sont les décisions prises par les opérateurs de service de DNS ou les

services de DNS qui peuvent avoir des conséquences indésirables quant à la disponibilité et à l'interopérabilité du système. Les TTL sont très importants, le temps de validité de la réponse. Les TTL trop longs ou trop courts peuvent présenter des problèmes ; il s'agit donc de chercher un TTL approprié, ni trop long, ni trop court.

Il y a aussi un scénario où les TTL trop courts sont utilisés et adaptés et il y a d'autres cas où les TTL doivent être longs. Mais les conséquences indésirables signifient qu'il faut évaluer de manière adéquate les risques pour s'assurer et pour bien connaître les conséquences des décisions que l'on prend en termes de décision de choix du TTL.

Si nous abordons la prochaine diapositive, nous voyons ici qu'on a eu un TTL sur un serveur faisant autorité et ce TTL assure que les utilisateurs finaux continueront à recevoir les réponses à leurs requêtes pendant un temps déterminé. Le registre cache est offert par le résolveur. Si l'attaquant peut intercepter la requête en séquestrant le nom de domaine en se servant des autres vecteurs dont j'ai parlé auparavant, la réponse malveillante est celle qui arrive dans la mémoire cache et l'utilisateur est toujours vulnérable. Il pourrait être exploité par cette vulnérabilité jusqu'à ce qu'on puisse récupérer la réponse correcte du serveur faisant autorité. Prochaine diapositive.

Nous avons déjà parlé du DNS comme vecteur d'attaque. Cela se rapporte à l'utilisation du DNS comme un canal caché. Nous pourrons voir ici comment on envoie les données sans les avoir filtrées. Nous parlons de canaux cachés et cela permet aux attaquants de s'infiltrer dans un système ou d'extraire des données de ce système vers l'extérieur ou sur le réseau.

Nous parlons aussi du déni de service. Pour tout opérateur d'infrastructure clé du DNS, cette attaque est un défi continu qui est toujours présent par suite du fonctionnement du protocole du DNS. Cela signifie que le service du DNS est vulnérable aux attaques de spoofing et à différents types d'attaque. Les attaques de déni de service peuvent perturber ou interrompre le travail d'un nombre bien plus important d'organisations que si la cible était l'opérateur de serveurs racine ou de service de registre. Ceci porte atteinte à une population beaucoup plus large que s'il ne s'agissait que d'attaques directes aux utilisateurs finaux.

Et sur ce, nous allons finir la description générale des vecteurs d'attaques. Et je cède maintenant la parole à l'un de mes collègues qui va parler des mesures d'atténuation.

DUANE WESSELS : Je vais parler de mesures d'atténuation.

Comme Gavin l'a déjà dit, il a parlé des attaques, nous avons consacré du temps dans notre groupe pour analyser comment on pouvait atténuer ces attaques et nous avons élaboré différents facteurs et stratégies. Il y en a qui ne sont pas arrivés au rapport final, mais je vais mentionner celles qui sont parvenues jusqu'au rapport final.

Nous avons consacré beaucoup de temps dans notre groupe au débat sur l'authentification et bon nombre des recommandations sur l'atténuation concernent le contrôle d'accès et d'autres questions liées à l'authentification. Ce que l'on peut faire de mieux pour que les ressources du DNS soient sûres et protégées, c'est d'utiliser le mot de

passe complexe. Il y a plusieurs cas où l'on utilise des mots de passe trop simples qui mettent en danger le DNS. Parfois, on utilise des mots de passe trop complexes, mais on peut se servir d'identification à usage unique ou des identifications multifacteurs. Lorsque les mots de passe deviennent plus complexes, on doit se servir d'un gestionnaire de mot de passe qui nous aide dans ce contexte au lieu d'essayer de nous rappeler chacun des mots de passe.

Le nous parlons de sensibilisation aux risques. Il s'agit de savoir la manière dont on peut compromettre les informations d'identification, comme les attaques de phishing. Nous parlons de l'utilisation de services qui empêchent les mots de passe faibles. Par exemple il pourrait y avoir des codes qui nous permettent d'évaluer si un mot de passe est suffisamment solide ou s'il respecte certains critères. Et il y a des bases de données où l'on peut chercher les mots de passe qui ont été compromis et nous pouvons toujours savoir que les délinquants peuvent avoir accès à ces mots de passe. Donc nous ne devons pas utiliser de mots de passe qui ont déjà été compromis.

Dans notre groupe, nous avons parlé aussi des solutions de recomposition en cas d'attaque, les manières dont les domaines et les titulaires de noms de domaine peuvent être vérifiés et validés par les clients lorsqu'ils présentent une candidature de registre. Prochaine diapositive.

Les mesures d'atténuation concernent la disponibilité, l'intégrité et la confidentialité. Il y en a qui sont vraiment très connues. Par exemple, pour la disponibilité, beaucoup d'entre vous savent qu'un seul point de défaillance unique n'est pas une bonne idée. Et souvent, on pense

à cela, les services de réseau ; il ne faut pas mettre tous les serveurs DNS sur le même réseau et sur le même centre de données. Bien sûr, il y a d'autres aspects, d'autres types de points de défaillance unique, comme par exemple le type de logiciel ou un seul type de matériel. Comme bon nombre de personnes ont compris après une attaque récente, on utilise aussi des services de DNS secondaires. C'est une bonne idée d'utiliser différentes plateformes parce que si nous n'en avons qu'une qui cesse d'opérer, le réseau est en défaillance.

Quant à l'intégrité, l'une des meilleures mesures d'atténuation est le DNSSEC ou le verrouillage du registre du côté de la vérification et du côté de la résolution qui se servent de la validation. Le verrouillage du registre et des outils semblables sert à empêcher le détournement des domaines. On parle aussi de l'utilisation de protocoles plus modernes comme le CDNSKEY et le CSYNC, qui facilitent la transmission du matériel du DNSSEC d'une zone enfant à une zone parent.

Quant à la vie privée, il y a eu un grand travail sur l'utilisation du DNS encrypté. Nous allons le voir de plus en plus souvent. C'est un très bon moyen de mettre en œuvre la vie privée dans le DNS. Prochaine diapositive s'il vous plaît.

Il y a d'autres mesures d'atténuation qu'il faudrait connaître, par exemple la surveillance. Nous pouvons avoir des abonnements aux services de protection de la marque si par exemple la marque de notre entreprise ou de notre domaine est enregistrée dans un autre domaine de haut niveau dans un autre registre. La transparence du certificat du moniteur, c'est un projet qui rend les demandes de certificat du SSL disponibles. Ce sont les services qui nous mettraient

en alerte si on a émis à un utilisateur légitime un certificat contre notre domaine.

Il y a aussi une autorisation de l'autorité de certification qui peut être mise dans la zone qui spécifie quelle est l'autorité de certification qui peut émettre des certificats pour ce domaine. C'est une bonne stratégie quant au routage RPKI. Et quant à l'authentification de l'utilisation du routeur optimisé, cela permet de protéger les réseaux de la fausse publicité. Cela peut être surveillé aussi.

Et pour ce qui est des organisations qui doivent mettre en œuvre un processus d'inspection des données qui passent dans leur réseau, elles devraient peut-être penser à des routeurs optimisés permettant l'inspection des paquets pour pouvoir savoir ce qui se passe dans les réseaux

Dans le cas des logiciels, on parle du besoin de compter avec les bonnes pratiques du cycle de vie et de développement des logiciels. On parle de la sécurité. Lorsqu'on développe un logiciel, il faut utiliser les meilleures pratiques pour qu'il soit actualisé et mis à jour et il faut corriger le logiciel régulièrement, non seulement du côté des opérateurs. Et il faut corriger le logiciel régulièrement pour éviter des problèmes.

D'autres mesures d'atténuation par rapport au contrôle d'accès incluent des architectures d'accès basées sur le comportement, par exemple Zero Trust, un de ceux qui commencent à être connus, la partition des services critiques en ligne, par exemple la séparation des services du DNS, de courrier électronique, ou de sites web, les mettre

dans différents systèmes ; si on attaque l'un d'eux, tous les autres ne sont pas attaqués. Il faudrait donc envisager des contrôles d'accès alternatifs ou plus restrictifs pour les informations ou les comptes sensibles.

Dans le cas où on peut partager les services, il faudrait restreindre l'accès au service DNS uniquement ainsi qu'aux ports DNS, le port 53, le port 853 avec TLS et peut-être le port 443 avec DNS sur HTTPS. Si l'on opère un résolveur du DNS pour être utilisé par des tiers, il faut s'assurer qu'ils aient un contrôle d'accès qui limite l'utilisation aux utilisateurs autorisés.

D'autres mesures d'atténuation pour le contrôle du point final et du réseau. Les antivirus pour les utilisateurs finaux existent depuis longtemps. Ils sont très utiles. On ne parle pas beaucoup des antivirus, mais on les utilise. Le contrôle strict de la sélection du résolveur DNS. Il y a un grand nombre de dispositifs qui reçoivent des serveurs DHCP par exemple, le serveur leur dit quel est le résolveur à utiliser et en général, cela fonctionne, mais il y a des moments où le malware ou d'autres vecteurs d'attaque peuvent changer le serveur de nom récursif qui est dans le dispositif. Il faut y faire attention, peut-être en bloquant ou en redirigeant le DNS via des résolveurs DNS ou des pare-feu DNS ou faire d'autres vérifications pour vérifier que le résolveur DNS soit correct. Et bien entendu, encore une fois, pour les organisations qui peuvent protéger leurs utilisateurs, utiliser un pare-feu est une très bonne idée parce que cela garantit que les utilisateurs n'arrivent qu'à des destinations appropriées et sécurisées.

Toutes les mesures d'atténuation dont nous avons parlé, on les a divisées dans les catégories suivantes. La plupart ont déjà été mentionnées, les défis d'identification, les contrôles d'accès, l'emprunt d'identité de ressources. C'est quelque chose que l'on a envisagé, aussi les vulnérabilités de code de protocole, le DNS comme vecteur d'attaque, le choix de l'infrastructure, le DNS comme vecteur d'attaque contre le DNS comme objectif d'attaque, le déni de service et les mécanismes de réponse aux incidents.

Je crois qu'avec ceci, j'ai fini mon exposé et maintenant, je passe la parole au prochain orateur.

MARC ROGERS : Très bien. Nous passons à la diapositive suivante maintenant.

Nous allons parler des recommandations élaborées à partir de ce que l'on a discuté au sein du groupe. Ceci a trait au système d'attaques et aux mesures d'atténuation présentées. Tout ceci est résumé dans ces cinq domaines où nous avons l'éducation par rapport à l'authentification et les autres domaines que vous voyez ici sur l'écran.

En premier lieu, on parle que l'ICANN devrait travailler avec d'autres organisations, le SSAC, etc. pour pouvoir développer des programmes d'exercices spécifiques afin de pouvoir voir les fonctions opérationnelles qui arrivent dans des situations d'incident pour trouver les fossés opérationnels existants. En faisant ceci de manière continue, toute cette brèche opérationnelle pourrait être identifiée et on pourrait faire le suivi au sein de l'ICANN pour pouvoir par la suite amener d'autres recommandations futures.

Il y a différentes recommandations. Tout d'abord, l'utilisation malveillante du DNS. Le panorama évolue en permanence. Les techniques d'hier ont évolué et elles sont différentes de celles de demain. Aussi, il y a différentes technologies qui peuvent être mises en place ainsi que différentes architectures du DNS. Nous croyons qu'il faut appliquer toutes les études au DNS pour voir quelles sont les manières d'utilisation malveillante et pour pouvoir anticiper justement.

La deuxième recommandation, c'est d'étudier les améliorations de la sécurité du DSN. Justement à cause de ces menaces qui changent en permanence, les améliorations à la sécurité doivent changer aussi. Il doit y avoir un programme pour enquêter les limites, les risques et les bénéfices de la sécurité du DSN. Ici, il y en a quelques-unes qui sont énumérées dans ce rapport. En général, l'utilisation malveillante du DNS, il faut faire le suivi, avoir un cycle de rétroalimentation où l'on peut identifier les fossés pour que ceci puisse se rétro-alimenter.

Pour ce qui est de l'authentification des sections précédentes, nous croyons qu'il faut aussi qu'il y ait une investigation des bonnes pratiques et des pratiques appropriées pour l'authentification. L'ICANN devrait faire des études ou un rapport sur les meilleures pratiques d'authentification lorsqu'on considère les différentes fonctions et risques dans le DNS.

Pour ce qui est des contrats et du financement, la recommandation, c'est que l'ICANN devrait travailler pour habiliter les parties contractantes afin d'adopter des améliorations à la sécurité pour l'enregistrement de noms de domaine. Et dans ce cas, on pourrait

nous assurer d'habiliter les organisations pour qu'elles mettent en place des mesures de sécurité bien plus robustes. Par la suite, nous avons les contrats et le financement et c'est une question très intéressante pour le groupe. Il y a beaucoup de perspectives différentes, quels sont les avantages, qu'est-ce qu'il faudrait adopter. Nous devrions dire à l'ICANN de mener un effort de collaboration pour travailler à la faisabilité du financement de cette recherche de défaillances. Il y a différentes manières. Tout ceci ne fonctionne pas dans toutes les organisations, alors ce serait un avantage d'avoir un programme de prime de bug concentré dans ce domaine et le logiciel qui permet d'identifier ces vulnérabilités. La question est très polémique, nous croyons donc qu'il faut faire une étude de faisabilité pour déterminer quelle est la meilleure approche, voir les coûts et l'efficacité en fonction des coûts et aussi quelles seraient les entités appropriées qui pourraient mener à bien cette activité.

Nous croyons aussi qu'il y a un besoin d'éduquer et de sensibiliser. Nous pensons que l'ICANN devrait élaborer et communiquer des programmes éducatifs en encourageant les parties prenantes du DNS à mettre à disposition les mécanismes d'authentification basés sur les normes appropriées pour toutes les interactions qui doivent être authentifiées ainsi qu'à informer ses parties prenantes des risques associés au système d'authentification. À la fois ici, on profite de l'ignorance, alors la sensibilisation et l'éducation permettent de passer à des schémas plus solides.

Le verrouillage du registre. L'ICANN devrait mener des efforts pour améliorer la documentation et la compréhension des fonctions de

verrouillage du registre, promouvoir leur utilisation le cas échéant et améliorer la compréhension des différences entre le verrouillage de registres de bureaux d'enregistrement. Les titulaires de nom de domaine devraient être en mesure de trouver des définitions claires de ce que ces caractéristiques fournissent. L'ICANN devrait envisager de faciliter la normalisation des exigences minimales pour le service de verrouillage du registre et du bureau d'enregistrement. Suivante s'il vous plaît.

Nous croyons qu'il existe le besoin aussi de créer une conscience sur les bonnes pratiques et l'ICANN devrait continuer à travailler avec des initiatives telles que MASN ou [KNS] pour mesurer et rendre compte de leur adoption et utiliser ces rapports pour cibler le matériel éducatif qui améliorera la sensibilisation à la sécurité de l'infrastructure. L'ICANN devrait prendre les meilleures pratiques issues de ces initiatives et s'assurer que les parties contractantes et la communauté de l'ICANN en soient conscientes. Là où les meilleures pratiques actuelles n'existent pas, l'organisation ICANN devrait encourager le développement et le déploiement de ces pratiques et promouvoir l'adoption de fonctionnalités d'amélioration de la sécurité de DNS, comme par exemple DMARC, SPF, TLSA, DANE, DNSSEC, etc.

La recommandation suivante a trait au verrouillage et au filtrage du DNS. L'organisation ICANN devrait créer des documents informatifs et éducatifs pour aider la communauté de l'ICANN, les parties contractantes et les autres parties intéressées à comprendre les risques et les avantages du verrouillage et du filtrage du DNS pour des

raisons de sécurité et de stabilité dans l'ensemble de la communauté de l'infrastructure du DNS mondial.

Pour ce qui est de la réponse aux incidents, l'organisation ICANN devrait, avec les parties concernées, encourager le développement et le déploiement d'un processus formalisé de réponse aux incidents dans l'ensemble de l'industrie du DNS qui permet une interaction avec les autres dans l'écosystème. Un tel effort devrait inclure la gestion des interventions en cas d'incident ainsi que le partage protégé des informations sur les menaces et les incidents ; ceci, pour s'assurer qu'il y ait aucun fossé, brèche ou lacune et qu'au cas où elles existeraient, ces lacunes puissent être identifiées.

On parle de la connaissance des canaux cachés. L'organisation ICANN devrait publier du matériel éducatif sur l'utilisation cachée des vecteurs d'attaques qui peut être considérée comme une utilisation malveillante du DNS qui nécessite une gestion comme d'autres problèmes d'abus du DNS.

Il y a des priorités que l'on peut sélectionner parmi toutes ces recommandations et en premier lieu, il y a la recommandation pour savoir quelles sont les bonnes pratiques d'authentification et en deuxième lieu, la recommandation 5, réponse aux incidents. Suivante s'il vous plaît.

Je passe la parole à Merike encore une fois.

MERIKE KÄO : Merci beaucoup.

Pour toute personne qui veut avoir des informations sur le groupe d'analyse technique et voir la charte, le plan de travail, les délais, les ordres du jour et les ressources, etc., vous pouvez vous rendre sur ce site. Comme on l'a mentionné, ce rapport sera disponible la semaine prochaine. Et je voudrais que vous anticipiez qu'il y a beaucoup de contenu très détaillé de ce que nous avons pu présenter dans ce temps si bref. Je crois que vous allez y trouver un contenu vraiment intéressant. Le PDG de l'ICANN trouvera vraiment des choses très intéressantes dans ce rapport.

Maintenant, je voudrais ouvrir la séance aux questions et réponses. Je ne vois pas de question.

WENDY PROFIT : Je crois qu'on a répondu par écrit à ces questions.

MERIKE KÄO : Si vous avez d'autres questions, vous pouvez les écrire dans la fenêtre de questions et réponses pour qu'on puisse y répondre.

Il y a une question : « Où peut-on trouver le rapport final ? » Le rapport final sera disponible la semaine prochaine sur le blog et d'après ce que j'ai compris sur le site du wiki que je vous ai montré sur la diapositive.

La question est : « Est-ce que ces questions et réponses accompagnent ce rapport ? » Est-ce qu'il y aura une transcription de tout ceci avec l'enregistrement ?

WENDY PROFIT : Je vais vérifier avec l'équipe MTS.

MERIKE KÄO : Merci de votre question, Donna.

Comme vous le savez, au cours des 18 derniers mois, nous avons consacré beaucoup de temps, mais vraiment longtemps à ce travail. C'était des experts qui avaient une expérience interfonctionnelle. C'était un travail excellent. Et je veux remercier chacun des membres de l'équipe ayant contribué à la rédaction de ce rapport.

En ce moment, je ne vois plus de question. Dans ce cas-là, je voudrais remercier tous ceux qui ont participé à cette séance de préparation. Et encore une fois, je vous prie de lire le rapport quand il sera disponible la semaine prochaine. Nous verrons après ce qui se passera après la lecture de ce rapport.

WENDY PROFIT : Nous avons une autre personne non identifiée qui pose une question dans la fenêtre de questions et réponses : « Quels sont les principaux motifs des attaquants ? Et de quels pays proviennent ces attaquants ? » Est-ce que quelqu'un pourrait répondre à cela ?

MERIKE KÄO : Les motivations peuvent être différentes. Il peut s'agir de personnes et il peut s'agir aussi de groupes de crime organisé. Et cela peut venir de n'importe quel pays. C'est simplement la nature du monde dans lequel nous vivons maintenant.

Parfait, donc nous allons finir cette séance. Je vous remercie vous tous de votre participation.

[FIN DE LA TRANSCRIPTION]