FR

ICANN84 | Réunion générale annuelle – ccNSO : Journée technique conjointe et séance sur l'utilisation malveillante du DNS
Lundi 27 octobre 2025 – 15h00 à 16h00 IST

CLAUDIA RUIZ

Dernière session de la Tech day. Je m'appelle Claudia Ruiz. Je suis avec ma collègue Andréa Glandon, responsable de la participation de cette séance. Cette séance est enregistrée, régie par le code de conduite des participants à la communauté ICANN, les normes de comportement attendu de l'ICANN et la politique anti-harcèlement de la communauté ICANN. Veuillez respecter les directives suivantes pour participer à cette séance. Je les publierai également dans le chat pour votre information. Pendant cette séance, les questions commentaires soumises dans le chat seront lues à haute voix, s'ils sont rédigés dans le format approprié comme indiqué dans le chat. L'interprétation pour cette séance comprendra l'anglais, l'espagnol et le français. Si vous souhaitez prendre la parole au cours de cette séance, veuillez lever la main dans Zoom. Lorsqu'ils sont appelés, les participants virtuels seront autorisés à réactiver le son sur Zoom, et les participants sur place utiliseront un micro pour prendre la parole. Veuillez indiquer votre nom pour le compte rendu, la langue que vous parlerez si vous ne parlez pas l'anglais, et parler à rythme raisonnable afin de permettre une interprétation précise.

Je cède maintenant la parole à Luis Diego Espinoza Sanchez, qui sera le président du groupe de travail technique de cette séance.

LUIS DIÉGO ESPINOZA Bonjour à tous. Merci Claudia. Je suis Luis Diego Espinoza. Je travaille avec .NA et nous avons une séance très intéressante aujourd'hui. Nous allons travailler avec Hafiz Farooq et Alan, et ils vont parler du DNSSEC et de la plateforme de DNSSEC. Je vais maintenant leur donner la parole. Donc plateforme de collecte de données DNSSEC. Vous avez la parole.

NAVEED BIN RAIS Est-ce que ça marche ? Bien, bonjour à tous. Bonsoir. Je suis Naveed, je vais vous présenter ce projet que nous avons lancé il y a peu. C'est un travail en cours de réalisation et nous attendons les commentaires de la communauté sur ce projet. Prochaine diapo.

Bien, ce projet s'appelle DNSexplore et il est sur dnsexplore.com. Donc je suis Naveed, je travaille comme directeur de ce projet et Farooq est un membre de mon équipe, et il est ici. Il est membre de la communauté de l'ICANN. Nous avons plusieurs membres qui travaillent sur ce projet, et l'idée de base est de mettre en place une plateforme DNS qui sera ouverte à la communauté afin de collecter des données sur les activités des DNSSEC pour internet, pour tous les domaines qui sont disponibles à tous les niveaux. Et ça va aider les chercheurs, la communauté ICANN et les membres, et d'autres

personnes qui sont intéressées par la définition de certaines brèches, de certains manques du DNSSEC.

Alors ici vous voyez ce projet qui se trouve à l'université d'Ajman. Je suis professeur à cette université, donc c'est dans la région des pays arabes, donc l'UAE. Nous travaillons tous les ans avec les élèves de cette sécurité. Il s'agit d'un projet financé par l'ICANN, qui vise à développer un système de plateforme de diagnostic et d'archivage du DNSSEC. Nous avons reçu une bourse de l'ICANN et donc nous travaillons sur la création de cette plateforme.

Actuellement, il y a des outils qui permettent d'identifier certains aspects, mais on ne sait pas très bien et comment archiver ces données pour voir les histoires, ce qu'il s'est passé au niveau du DNS, l'évaluation au niveau du DNSSEC et autres problèmes qui peuvent surgir concernant le DNSSEC.

Alors voilà, ici vous voyez certaines caractéristiques de ce projet. Il y en a beaucoup d'autres, mais j'en présente seulement quelques-unes. Ici, donc nous voulons analyser 600 millions et quelques de domaines internet qui vont inclure les gTLD et ccTLD, et ce projet vise à leur fournir un soutien de la part de notre serveur de façon à ce qu'on ait un serveur qui travaille en permanence et qui fournisse ces informations et qui puisse identifier les manques et dans la mise en œuvre du DNSSEC.

Actuellement, nous avons une estimation de 10 millions de domaines par jour que nous pouvons donc analyser grâce à notre serveur et nous pensons être capable de retenir, ou d'archiver, des

données concernant le DNSSEC sur un an. L'objectif de cet outil est qu'il soit gratuit pour la communauté internet et pour la communauté ICANN, donc tout le monde peut l'utiliser, avoir accès à ces données sur cette plateforme. Cette plateforme va fonctionner, il va y avoir bien sûr un système de licence, mais va fonctionner gratuitement.

Alors quels sont les bénéficiaires de ce projet ? J'en ai ici présenté quelques-uns, cela inclut la communauté internet, les bureaux d'enregistrement gTLD, les opérateurs de registres, les chercheurs, le secteur académique, les experts de sécurité cybernétique, les ccTLD, et cætera.

Par conséquent, si on avance un petit peu, cela va nous aider à identifier les statistiques du DNSSEC de la mise en œuvre du DNSSEC, et des manques qui existent au niveau des TLD, des domaines de deuxième niveau, et autre. Et nous voulons fournir tout cela, et fournir une carte avec un graphique du monde entier. Cela figure sur notre site, et ce site est déjà actif. C'est un site en cours de réalisation, donc pour le moment, nous pouvons fournir certaines informations seulement. Et nous en sommes notre objectif est d'avoir des statistiques de la zone concernant les ccTLD et inclure tout cela, et TLD aussi inclure tout cela sur notre plateforme.

Voilà les jalons de ce projet. Nous en sommes à la phase d'appel d'offres de matériel, nous avons un laboratoire qui devrait commencer à fonctionner en 2026, et le système de recherche du

DNSSEC devrait fonctionner en février en 2026. Nous faisons des analyses des domaines internet. Ce processus devrait nous permettre de commencer à travailler dans ce secteur entre juillet 2026 et octobre 2026, et nous espérons donc avoir toutes les caractéristiques disponibles sur notre plateforme par la suite.

Voilà une architecture générale de ce laboratoire de recherche avec quelques serveurs qui fonctionnent et qui fournissent de la sécurité avec des systèmes de backup et des systèmes de protection qui devraient fonctionner en permanence, de façon à fournir ces services. Je vais m'arrêter ici, et je vais laisser mon collègue continuer la présentation, et ensuite il vous présentera une démonstration.

HAFIZ FAROOQ

Merci beaucoup. Je suis Farooq. Je suis membre de la communauté internet et membre du comité NomCom. Alors, cette architecture du système, comme je l'ai dit, nous allons travailler sur un système qui va nous permettre de travailler sur internet, de faire des recherches. Ce système sera actif 24 heures sur 24, 7 jours sur 7, et ici vous avez le serveur cache du DNS.

Nous allons alimenter les domaines et toutes ces données passeront dans ce système de crawler, et à travers le DNSSEC.

Bien, alors la vérification. Il s'agit ici de flux de travail de DNSSEC, qui travaille avec tous les domaines. Vous pouvez le faire sur notre site internet, vous pouvez spécifier les noms de domaine, vous

pouvez le faire avec des domaines de deuxième niveau, de premier niveau, commencer à vérifier le passer au niveau supérieur TLD, si cela existe, et vérifier tout cela, donc ça va faire des vérifications de base, puis les passer au niveau supérieur. Cela va vérifier que l'on a la norme de sécurité qui s'appelle Secure. C'est similaire à des projets qui existent déjà comme VeriSign, DNSViz, et autre, mais puisque nous travaillons avec ce système de crawling, nous fournissons l'histoire des données, ce qui fournit un bon niveau de sécurité.

Alors si vous pouvez me permettre d'être co-hôte, je voudrais vous montrer une démonstration ici de ce système. Alors si je peux partager mon écran ? Merci. Ici, vous voyez, nous avons l'arbre de ICANN.org, qui est signé. Nous commençons par la root ici, qui est déployée avec des clés actives, la KSK1, la KSK2. Ici vous avez le préalable 2326, et ici c'est le nouveau. Et ici c'est celui qui est actif. Donc nous allons vérifier le prochain niveau. Et ici, vous le DS pour la zone racine, et si nous continuons à descendre, ici dans la zone nous avons ces ZSK qui sont déployés. Vous pouvez prendre une clé en particulier, vous allez voir les métadonnées en particulier, et les enregistrements et le statut de cette couche en particulier est signé. Vous le voyez ? Ici. Si vous continuez à descendre, à ce moment-là vous allez voir le prochain niveau qui est ICANN.org, donc ici vous avez KSK, ZSK, qui sont signés, et voilà les enregistrements individuels. Dans cette zone en particulier, voilà un exemple de domaine signé.

Et on parle de comparer à un autre domaine, que je vais vous montrer. Donc serverfault.com, c'est le nom du domaine. De nouveau ici, tout va bien, tout marche bien jusqu'à ce que l'on arrive au niveau qui est severfault.com. Et ici, vous voyez qu'il n'y a pas d'enregistrement des DS dans cette zone pour ce domaine en particulier, et donc il est non signé. Donc une caractéristique intéressante que nous allons fournir, et c'est une ligne de temps qui va vous permettre de reculer dans le temps. Vous allez voir, par exemple, cette zone en particulier, il y a trois mois, vous pouvez faire un suivi de l'histoire en particulier, voir ce qu'il s'est passé à cette période. Et nous travaillons aussi sur d'autres projets, et une fois que ce projet sera terminé, vous verrez beaucoup de données et de statistiques concernant les données que nous avons collectées jusque là.

Voilà j'en ai terminé, si vous avez des questions, je peux y répondre. Merci beaucoup.

LUIS DIÉGO ESPINOZA Est-ce que vous avez fini ?

HAFIZ FAROOQ Oui, j'ai fini.

LUIS DIÉGO ESPINOZA Merci. Nous sommes un peu en avance.

ALEXANDER MAYRHOFER Alexander au micro. Est-ce que vous êtes au courant de l'ouverture de ce projet avec ce robot d'indexation pour Intel, et ça peut utiliser de nombreux noms de domaines, sur une base quotidienne, sur une base de nombreux noms de domaines qui sont collectés ainsi. Donc est-ce qu'il y a des archives DNSSEC également ? Non j'y pensais, ce n'est pas moi qui aie fait ça.

HAFIZ FAROOQ Donc je ne suis pas au courant, mais si vous collectez des données, on peut vous parler en aparté et travailler quelque chose. Nous collaborons avec quelques projets déjà, des projets existants. Je crois que c'est le SecSpider, donc l'araignée du DNSSEC de l'université George Mason, du docteur Éric. Et on travaille beaucoup avec eux sur ces données. Donc nous sommes très intéressés d'utiliser ces données, donc ça c'est l'indexation qui se fait au début. Maarten vous voulez rajouter quelque chose ?

MARTEEN AERTSEN Oui, je suis aussi d'une autre université. Je connais le projet de l'université de Twente.

LUIS DIÉGO ESPINOZA Merci. D'autres questions de la part de l'auditoire ? Tr-s bien. Tom ?

PETER THOMASSEN Non c'est Peter en fait, de SSAC. Donc j'ai regardé l'illustration de la démonstration. C'est tout à fait intéressant, et je crois que la

version alternative fonctionne bien. Donc vous avez la KSK, vous avez parlé de la KSK, vous avez parlé des clés de chiffrement. Je voudrais savoir comment cela est utilisé ? Donc je crois que c'était un petit peu heuristique comme désignation, mais néanmoins tout à fait intéressant, je crois que cela pourrait être qualifié un petit peu différemment.

HAFIZ FAROOQ Donc je n'ai pas bien compris la question, donc si vous pouvez répéter s'il vous plaît ?

PETER THOMASSEN Donc on n'a pas beaucoup de temps, mais je vous contacterai personnellement. Mais non je voulais dire que dans la présentation, vous avez différentes clés, donc par exemple icann.org a la KSK, les clés de chiffrement. Et ce n'est pas possible de voir s'il y a une ZSK également utilisée comme KSK parce qu'il y a différent chiffrement, et ces clés ouvrent différents dossiers, donc en général c'est difficile à dire si une clé est utilisée d'une manière combinée ou pas. Et donc dans votre illustration, il m'a semblé que c'était étiqueté un petit peu différemment, et c'est pour cela que je posais cette question, et je pense qu'il faut être un petit peu prudent et bien étiqueter cela.

HAFIZ FAROOQ Donc oui, il y a différentes clés qui ont la clé du DNS, la ZSK, KSK également, donc il y a différentes identités 256, 257, c'est pour cela qu'il y a une différence.

PETER THOMASSEN En ce qui concerne le drapeau SCP, je pense que c'est utilisé un petit différemment pour les opérateurs du DNS, donc c'est un protocole qui n'est peut-être pas pertinent au niveau de cette clé 256, et je pense que ce n'est pas strict.

HAFIZ FAROOQ Oui oui, je pense que vous avez raison, tout à fait.

LUIS DIÉGO ESPINOZA Y a-t-il d'autres questions ? Un commentaire dans le chat ? Bon, on reviendra là-dessus plus tard. Donc, nous avons un petit peu de temps. Nous pouvons passer à la prochaine présentation, ensuite on reviendra aux questions. La prochaine présentation sera sur Cascade, donc système de signature DNSSEC en lequel vous pouvez avoir confiance, de la part de Marteen Aertsen, des laboratoires NLnet.

MAARTEN AERTSEN Oui, merci beaucoup. Maarten Aertsen au micro. Aujourd'hui je vais vous présenter Cascade, un nouveau projet qui est donc le successeur d'un DNSSEC ouvert. Donc je voudrais pour NLnet Labs, organisation à but non lucrative d'Amsterdam, et nous avons

célébré notre 25e anniversaire, et ce que nous faisons dans ces laboratoires c'est que nous travaillons à des logiciels Open Source pour la communauté mondiale.

Donc nous participons activement dans l'IETF, et dans ce groupe de travail de génie internet, donc aujourd'hui je parle au nom de l'équipe Cascade d'Amsterdam, et si vous étiez à DNS Org à Stockholm, je reconnais certains visages, et bien vous avez vu peut-être déjà ce contenu, parce que ça a été délivré par un collègue, Aria. Mais nous pensons que c'était extrêmement important de parler de cela à la ccNSO.

Donc, dites-moi si vous connaissez bien Cascade, comment ça fonctionne pour vous, et si vous en êtes satisfaits.

Je vais parler, tout d'abord, de Cascade, expliquer pourquoi ça existe, et je vais parler des critères pour Cascade. Je vais vous montrer l'architecture, j'espère que ce sera utile pour mieux comprendre comment opérer, faire fonctionner Cascade. Et vous serez bien situés pour essayer ce logiciel Cascade, Open Source, et on verra ce que nous apporterons par la suite à Cascade. Puis je pourrais répondre à vos questions avec plaisir.

Donc quelques nouvelles du laboratoire NLnet avec Maarten, Philip, Aria, nous avons développé avec Rust, on a utilisé en 2024 une bibliothèque DNS basée sur Rust, pour domaines, et là on peut écrire des logiciels DNS sophistiqués et on a développé des règles pour cela. Et la bonne nouvelle, c'est que nous sommes maintenant prêts à plus de sophistications à nos applications DNS

grâce à Rust. Donc merci aux techniciens qui nous ont aidés dans tout ce travail.

Nous avons déjà un DNSSEC, l'OpenDNSSEC qui a 15 ans d'existence maintenant, et qui a été en collaboration avec de nombreuses personnes. Certaines de ces personnes sont ici, et ça a très bien fonctionné, et vraiment on est très fier d'avoir servi une communauté en travaillant sur les codes du DNSSEC. Le DNSSEC est plus accessible maintenant, mais ces dernières années, nous vous avons écoutés, et en tant qu'opérateur, ça ne suffit plus le DNSSEC ouvert. Il y a des zones qui ont évolué, donc on a essayé de mieux comprendre ce que l'on pouvait faire pour le développer. On a écouté par des questionnaires ce que pensaient les opérateurs.

Les personnes effectuant les signatures ne communiquent pas beaucoup. Elles ne communiquent pas ce qu'elles font, pourquoi elles le font et il y a un manque de confiance au DNS. Il faut vérifier les signatures, et continuellement vérifier les signatures. Donc c'est un risque qui existe. Il y a une forte disposition d'avoir plusieurs personnes qui signent, ça peut être problématique à gérer. Donc il y a une accumulation de problème, il y a une seule personne dans l'équipe qui va être chargée de la signature ; et sans cette personne la structure va s'écrouler.

Et donc nous avons bâti un nouveau système de signature DNS qui s'appelle Cascade, pour le DNSSEC. Et ça, c'est un système dédié. L'objectif est uniquement pour ces signatures, avec Rust comme je

l'ai dit. Cela permet d'avoir les avantages du DNS ouvert et ça répond aux besoins des opérateurs d'aujourd'hui.

Ce mois-ci, nous avons lancé une version alpha de Cascade, que vous pouvez essayer. Certains ont déjà expérimenté avec Cascade, et on apprécie beaucoup le retour de votre part. Nous avons plusieurs versions alpha pour améliorer continuellement donc Cascade. Donc, en 2026, on va avoir une version prête à la production et ça va être possible de l'utiliser dans vos zones. En ce qui concerne le DNSSEC ouvert, le 3 octobre, nous avons publié un plan de retrait de l'Open DNSSEC et le remplacement avec Cascade. Je vais pas beaucoup parler de cette annonce, mais n'hésitez pas à me poser des questions à ce sujet. Il y a un lien hypertexte à partir de cette diapo.

Alors, comment est conçu Cascade ? Nous avons passé pas mal de temps à réfléchir à la manière dont cela aura un impact sur l'architecture du DNSSEC, et j'espère pouvoir vous montrer un petit peu que nous répondons à des besoins d'une manière significative, donc le plus important c'était d'écouter les utilisateurs. Et l'équipe seule aurait bâti quelque chose peut-être très divertissant, mais qui n'aurait pas beaucoup servi la communauté. Donc on a vraiment dû écouter la communauté des opérateurs, des utilisateurs, pour concevoir Cascade. Et on a pu parler avec 16 opérateurs, tout en concevant Cascade, et on a pu poser des questions, et donc faire évoluer ce système.

Et là je reviens à une diapo que vous avez déjà vue : revoyons une nouvelle fois cette liste. Les personnes effectuant les signatures ne communiquent pas beaucoup, on ne peut pas leur faire totalement confiance, c'est un travail au quotidien. C'est vraiment comme un couple qui va mal, et ça peut s'écrouler à tout moment. Il y a différents ensembles pour Cascade.

Donc la priorité, c'est la confiance. Ça ne veut pas dire que vous devez avoir confiance tout de suite. Si vous continuez à l'utiliser, c'est d'avoir une relation qui soit sous le signe de la sérénité. Vous n'êtes pas toujours d'accord avec ce qu'il se passe, parfois vous voulez travailler manuellement, pas toujours automatiser les tâches, et vous voulez vous assurer que ça fonctionne bien.

En ce qui concerne les caractéristiques concrètes, on a voulu avoir une interface détaillée, solide, et contrôler toutes les actions automatiques. Nous avons également un bon soutien pour une forte disponibilité, pour avoir plusieurs personnes pouvant effectuer les signatures à l'avenir. Donc on ne veut pas que les opérateurs soient limités par Cascade, pas du tout. Nous avons des interfaces de programmation d'application, des API qui sont complètes, avec des documents d'aide qui sont également complets et qui intègre des outils modernes, on veut un soutien professionnel, et on veut que les infrastructures critiques qui soient beaucoup mieux conçues, dirons-nous.

Donc nous avons bâti cela, et nous pouvons maintenant en parler. Qu'est-ce que nous avons conçu au niveau de Cascade ? Et bien

c'est quelque chose qu'on pouvait télécharger, et qu'on peut télécharger, et cela voulait dire qu'il fallait écrire beaucoup de codes. Et les éléments essentiels de Cascade, c'est un système de signature DNS et un responsable de clé, un mécanisme pour approuver les zones et un soutien à ce niveau également. Pour qu'il y ait des interactions fortes avec ce système, on a développé un API, interface de programmation d'application HTTP pour contrôler tous les éléments, et on a une architecture autour de ce pipeline de signatures, vous en avez entendu parler à Prague avec Philip. Et véritablement, nous avons également Internet Stifelsen qui a beaucoup travaillé à cela. Nous avons également pris le temps de développer les statuts et les résultats avec un statut de résultats avec matériel du CLI et de IP.

Donc voilà à quoi cela ressemble. Je vais vous donner un instant pour regarder cette architecture sur la diapositive que vous avez à l'écran. Et Cascade c'est dans un pipeline de zones que l'on va le trouver, donc vous avez les fichiers non signés qui arrivent sur la gauche, et il va y avoir un serveur un nom primaire comme NSD et ensuite tout se passe entre ces deux points, ce qui est bleu sur la diapo. Cascade a donc des éléments qui chargent la zone. Il y a une signature DNSSEC et il y a un responsable de clé qui fait le travail de signature de la zone, et donc tout ce travail est réalisé de cette manière avant et après la signature. Cascade revoit tout cela avant la publication de résultat. Donc vous pouvez avoir une logique de validation qui soit renforcée et vous avez une plus de confiance à portée grâce à cascade dans ce pipeline, et vous pouvez donc vous

assurez qu'il n'y ait pas de donnée invalide ou corrompue, vous avez le temps de savoir ce qu'il se passe et ce qui peut poser problème dans ce pipeline.

Donc voilà un aperçu de ce système de Cascade, et de sa pipeline zone. Alors qu'est-ce que nous allons faire ensuite ? Nous aimerions d'abord entendre votre opinion, nous voudrions comprendre exactement ce dont vous avez besoin, et la production que vous voudriez avoir de notre part durant la première partie de 2026. Ce que nous souhaitons maintenant c'est de travail avec des personnes qui travaillent sur des zones spéciales, voire s'ils peuvent l'utiliser. C'était la demande que j'ai reçue il y a quelques heures de la part de l'équipe. Si vous pensez que votre zone fonctionne bien, entrez en contact avec nous et nous serons ravis de vous présenter ce que nous sommes en train de construire durant cette première phase.

Ensuite, avant de conclure, un petit détour, nous vous demandons de nous aider à remplacer le DNSSEC ouvert. Nous allons faire des modifications à ce DNSSEC ouvert pendant 2 ans de plus, et ensuite c'est la fin de vie de DNSSEC. Nous savons que ce logiciel est utilisé partout dans le monde et dans beaucoup d'endroits, et qu'ils n'ont jamais échangé avec nous, ni avec les développeurs de ce système. Par conséquent, c'est le moment de planifier le futur de façon à savoir comment passer d'une infrastructure à l'autre. Nous travaillons sur son successeur, mais on aurait besoin de votre aide. C'est-à-dire d'abord on a besoin de finance, d'aide financière, parce que notre projet à long terme nous permet d'avoir un

contrat, mais quand nous travaillons sur un contrat comme par exemple, Cascade, nous avons construit Cascade depuis le début, nous n'avions pas de contrat de soutien à cette époque-là, et le futur devrait nous permettre de faire des recherches à long terme sur des finances, avec des ressources. Nous avons 6 personnes qui travaillent sur Cascade actuellement, et vous allez pouvoir utiliser Cascade gratuitement, comme nous l'avons toujours fait avec nos logiciels, mais le développement n'est pas gratuit. Donc nous voulons financer ces efforts. Nous les finançons par nos réserves, c'est un choix, parce que nous pensons que le DNSSEC doit être remplacé, nous croyons dans la diversité des logiciels, et nous cherchons des cofondateurs pour nous aider à avancer dans ce projet puisque ce type de projets ne peut pas être financé sur des réserves seulement. Nous avons besoin de davantage de finance. Donc si vous ça vous intéresse, si la diversité des logiciels vous intéresse, n'hésitez pas à nous joindre. Nous avons déjà plusieurs partenaires avec qui nous sommes en train d'échanger, mais nous pourrions en avoir davantage.

Après ce petit détour, je vous remercie pour votre attention. N'hésitez pas à joindre vos collègues internationaux qui parlent déjà avec nous pour le remplacement du DNSSEC ouvert, et essayez Cascade dans vos systèmes, dans vos laboratoires, si vous ne l'avez pas fait encore. Vous pouvez en savoir plus à propos de Cascade sur la gauche, vous avez des visios, des documents et la source. Tout cela est donc à votre disposition. Et je suis maintenant disposé à répondre à vos questions.

LUIS DIÉGO ESPINOZA Merci beaucoup. Est-ce qu'il y a des questions ? Allez-y.

YAZID AKANHO Merci. Yazid de la participation de l'ICANN Engagement. Alors vous avez parlé de la validation de zone que le système pourrait réaliser. Est-ce que vous avez l'intention d'avoir différents types d'outils de validation de zone ?

MARTEEN AERTSEN Oui, je crois que j'ai une diapositive là-dessus. Laissez-moi regarder. Oui, nous avons ce concept de review. Ça fait partie du document que nous utilisons aujourd'hui. Aujourd'hui nous utilisons ce système pour vérifier la zone signée, et c'est justement un petit script, mais ça permet d'être flexible : vous pouvez ou bien faire un transfert de zone du serveur DNS qui est sur le pipeline, vous pouvez l'identifier ; ou bien vous pouvez aussi le faire avant le fichier, exécuter un script de type shell. Et je pense qu'on peut explorer cela d'autres façons, mais ce que nous voulons, c'est avoir ici votre logique dans le pipeline à différentes étapes.

Donc maintenant les étapes que nous avons identifiées c'est qu'avant de signer et après la signature de la zone. Et si vous ne faites pas de signatures, ce concept est quand même assez utile. Donc je pense que c'est une réponse et un exemple que je peux vous fournir.

LUIS DIÉGO ESPINOZA Bien, nous avons quelques minutes encore si vous avez des questions. Et on peut passer à la prochaine présentation. Nous allons donner la parole maintenant à Nathan Alan, directeur engineering, qui va nous parler des blockchains et du risque de collision. Allez-y.

NATHAN ALAN Merci beaucoup. Bonjour à tous. Je vais vous expliquer un petit peu ce dont nous allons parler aujourd'hui. Nous allons remonter dans le temps. L'année dernière, nous avons travaillé avec l'AFNIC et nous avons fait des recherches sur l'utilisation de la blockchain et d'identificateurs blockchain.

Nous avons pris une série de données. 11 millions d'identificateurs répartis sur 6 millions d'entre eux étaient des identificateurs et des identificateurs de premier niveau des enregistrements qui avaient été fait dans la blockchain et on a essayé d'établir avec AFNIC, essayer de comprendre ce qu'il se passait dans cet espace où tous les enregistrements sont faits du point de vue des marques ou de propriétaires de marques, de façon à ce qu'ils comprennent ce qui est enregistré, comment cela peut les affecter dans le futur.

Le deuxième projet que nous avons révisé, c'était une cartographie des différents fournisseurs qui offrent des enregistrements de domaines blockchains. C'est une recherche qui nous permet de voir ces fournisseurs, où est-ce qu'ils se trouvent, quels sont les

services qu'ils offrent ? Et aujourd'hui, je vais vous présenter une analyse que nous avons faite qui couvre ce secteur clé de ces enregistrements et des données que nous avons.

Alors les identificateurs de blockchain vont dépendre des services qu'utilisent certains fournisseurs. La capacité que d'utiliser des portefeuilles de cryptomonnaies, des transactions, d'autres offrent d'autres services similaires aux DNS pour poster des contenus et ce type de chose. Donc, comme je l'ai dit nous avons 11 millions et quelques d'enregistrement et nous nous sommes centrés sur les enregistrements de deuxième niveau seulement de façon à ce que ces enregistrements de deuxième niveau ont été analysés dans cette recherche, et la recherche nous a permis d'analyser les enregistrements et faire une cartographie de ces enregistrements, et de le relier à l'utilisation malveillante du DNS. Et pour cela, nous avons utilisé un système Global Signal Exchange. Pour ceux qui ne connaissent pas, il s'agit d'une organisation à but non lucratif qui est conçue pour partager des renseignements de menaces à travers le secteur du nom de domaine.

Donc nous avons 45 différents feeds de renseignements qui passent par des plateformes, voire quelles sont les parties prenantes qui opèrent avec le DNS pour essayer de créer des sauvegardes, de protéger ces systèmes.

Donc dans le cadre de cette partie de la recherche que nous analysons, nous avons une approche avec six perspectives différentes concernant ces données. Comment les autres

enregistrements vont donner lieu à des corrélations entre pas de rapport d'utilisation malveillante du DNS et comment elles sont utilisées ? Ce que vous pouvez les utiliser certaines de ces enregistrements pour héberger du contenu ? Est-ce que certains vont représenter ou vont violer des noms de marques ? On a aussi analysé la compatibilité des navigateurs : quels sont les navigateurs qui étaient identifiés compatibles avec des navigateurs courants ? Quels étaient les plugings ? Quels étaient les résolveurs DNS qui étaient installés pour les utiliser, pour les faire fonctionner ?

Ensuite, la résolution de règlement de différends. Alors, nous avons analysé cela, un peu d'un point de vue des marques parce qu'il y a eu des enregistrements de noms de marques, est-ce qu'il y a des mécanismes pour ces noms de marques et pour faire valoir leurs droits.

Ensuite, en termes d'utilisation malveillante de ces identificateurs de blockchain, 6,4 millions, nous avons comparé les menaces de Global Signal Exchange. Les données que nous avons reçues avec 500 millions de points de données qui contenaient des menaces potentielles d'utilisations malveillantes du DNS. Hameçonnage, logiciel malveillant, et autres menaces.

Nous avons constaté que 10 % correspondaient à des utilisations malveillantes et à des rapports pour abus et utilisation malveillante. Ce qui a donné 670 mille identificateurs. Alors si on regarde la violation, concernant les noms de marques, c'est un peu

inférieur. Beaucoup de fournisseurs de blockchain vont essayer de prévenir des enregistrements de marques ou de marques ciblées. On a constaté que les enregistrements qui étaient ressemblants, qui pouvaient porter à confusion, par rapport à des noms de marques et on avait les données d'enregistrement. On n'a pas pu qui était celui qui avait fait cet enregistrement. Donc c'était difficile de savoir quand cela correspondait. On ne savait pas si c'était le titulaire de la marque ou pas. Et ça, il faut le dire.

En termes de règlement de litige, il n'y a pas beaucoup de mécanismes disponibles. C'est difficile, il faut le savoir. Pour les noms de marques, il est difficile de modifier un enregistrement de blockchain, et on sait que certains fournisseurs essayent de fournir des mécanismes de blocage quand il y a un problème, et une violation des droits. Nous voulons essayer de comprendre s'il y a des enregistrements sur une blockchain, s'il y a eu un cas bien révolu du DRP.

Nous avons analysé tous les cas de toutes les affaires liées au UTRP pour essayer de les analyser et voir si il y avait eu des résolutions réussies. Et on a constaté que 1456 identificateurs de blockchain avaient donné lieu à des plaintes, et à des transferts de l'UDRP avec succès.

Donc il y a ici certaines répétitions, mais je dirais que les marques les plus affectées comprennent Google, Amazon, Instagram, et c'est ce qui participe à ces procédures du DRP.

Donc nous avons eu un projet où nous avons trouvé 13 % des fournisseurs de la blockchain qui offrent un soutien avec Brave ou Opéra au niveau des navigateurs. Et donc, ça va s'accroître avec le temps, mais il y a une résolution qui est faite avec des extensions, c'est comme cela que c'est utilisé ces mécanismes d'extensions pour le DNS. Et il y a un lien, notamment avec le nuage et il y a certains contenus qui sont résolus de cette manière.

Donc pourquoi c'est important et qu'est-ce qu'on va faire à l'avenir pour améliorer cela ? Et bien, je l'ai dit dès le début, cette recherche a été basée sur un aperçu des enregistrements blockchain, et ce qu'on voudrait faire, c'est d'avoir notre ensemble de données d'enregistrements pour avoir un historique. Et pour ceux que cela intéresse, on peut expliquer quels sont les types de robots d'indexations pour les marques, pour les noms de domaine. Et c'est important qu'on ait un dialogue au niveau de la communauté, entre nous, sur ces problématiques. On est là pour vous aider, pour mieux comprendre l'espace de la blockchain et son rapport avec les différents numéros, et les résultats de ces recherches. Je pense que cela sera intéressant pour les identificateurs, donc il y aura utilisation, notamment en ce qui concerne les enregistrements. Cela va permettre de mieux comprendre ce qui est utilisé activement et par exemple, les cryptodevises, les transactions de ce types.

Donc ça, c'est simplement la surface des choses, mais je crois que nous avons déjà observé des enregistrements de blockchain à ce sujet. Si vous voulez en savoir plus pour comprendre les risques de

collision avec les noms, sur notre site web vous pouvez avoir accès à cela. Nous avons donc ces identificateurs de la blockchain qui sont en rapport avec les noms de domaines.

LUIS DIÉGO ESPINOZA Merci beaucoup. Est-ce qu'il y a des questions de la part de l'auditoire ? Oui, allez-y.

BENOÎT AMPEAU Ce n'est pas une question, mais c'est un commentaire. Benoït Ampeau de l'AFNIC. Donc je reviens à ce qui a été dit plus tôt, et Nathan c'est important, en effet, d'avoir cette première analyse, mais les choses évoluent. Et vous parlez de l'intégration du DNS, nous voyons en effet plus d'intégration dans les navigateurs. C'est tout un écosystème qui évolue, n'est-ce pas.

LUIS DIÉGO ESPINOZA Merci. Est-ce qu'il y a d'autres commentaires ou questions ? Oui, la dame là-bas ?

GEORGIA OSBORNE Bonjour Nathan, Georgia Osborne, au micro, de la SSAC. J'ai une question en rapport avec les indicateurs. Est-ce que vous avez plus à nous dire au niveau de la matrice utilisée et comment sont obtenus les résultats d'une manière plus spécifique ? Et je sais que

vous avez beaucoup parlé de la matrice, vous avez parlé d'utilisation malveillante du DNS. Oui c'est sur cette diapo.

NATHAN ALAN Alors, nous ne savions pas véritablement à quoi nous attendre, s'il y avait des corrélations véritablement entre les enregistrements blockchain et les enregistrements DNS pour les utilisations malveillantes. Et bien, c'est difficile à dire, je ne sais pas à quoi m'attendre. 10 % des enregistrements qui vont être indiqués comme étant abusifs étaient déjà enregistrés sur la blockchain. Ça ne veut pas dire que c'est abusif, ce n'est pas ce qui était dit, parce qu'il y a des enregistrements légitimes à ce niveau et on n'a pas assez de données ou d'informations sur l'utilisation de ceux-là. Et on aimerait véritablement continuer à creuser à ce niveau.

LUIS DIÉGO ESPINOZA Oui, vous avez une question. Allez-y.

THOMAS CLOWES Thomas, Ethereum. Donc vous avez parlé des recherches qui ont déjà été effectuées, et c'est assez fascinant. Il y a des limites techniques, en effet, mais il y a toujours des recherches qui sont effectuées. Nous aimerions nous allier avec l'ICANN et continuer à vous aider si vous avez besoin de soutien pour poursuivre votre recherche.

LUIS DIÉGO ESPINOZA

Est-ce qu'il y a d'autres questions ? Très bien, donc nous avons la possibilité d'applaudir nos brillants intervenants et nous pouvons avancer aux différentes remarques maintenant. Oui, désolé, allez-y.

JAROMIR TALIR

Oui, merci beaucoup, Diégo, c'est un honneur. Nous allons conclure cette séance et résumer ce que nous avons appris aujourd'hui.

Donc dans notre premier block, aujourd'hui, nous avons commencé avec une présentation d'étudiants de l'université de Delft. Ils ont présenté un logiciel sur le NTP. On a parlé des différents protocoles, et de temps de réaction, et ils ont présenté leurs recherches sur l'influence des données et différentes mesures des données. Le logiciel permet donc d'utiliser le serveur NTP, voir à quel niveau de performance il se situe. On a eu des conseils pour améliorer cela et l'automatisation était intéressante parce qu'il y avait tout un répertoire qui était utilisé et cela est tout à fait intéressant pour la communauté.

La deuxième présentation, nous avons parlé des directives pour l'automatisation du DNSSEC. L'objectif c'est d'accroître l'automatisation DNSSEC et de soutenir la manière dont cette automatisation peut arriver dans l'espace ccTLD également. Et donc le groupe d'ingénierie de l'internet se penche là-dessus. Ces lignes de conduite sont en mesures, avec la qualité, en rapport avec la validité des mesures de sécurité, le rapport sur la transparence,

les fichiers d'enregistrements et la communauté peut continuer à travailler à cela et commenter sur ces sujets. Donc si cela vous intéresse, vous pouvez continuer à travailler avec nous.

La troisième présentation, c'était de Neil Dundas. On a parlé de différents rôles des registres et l'importance des données pour les rapports pour la transparence également et pour des décisions commerciales basées sur les données. Donc il y a eu des expérimentations qui ont été faites avec des étudiants de l'université de Pretoria. Il y a eu des partenariats qui ont été menés et il y a un pipeline qui a été conçu. Il y a donc un entreposage des données et on a travaillé sur l'interface de programmation d'application API et sur les différents tableaux de contrôle.

Dernière présentation était consacrée au laboratoire DNSSEC. Cela est géré par l'ICANN et c'est un environnement où il y a différents ateliers, auxquels on peut participer, et le laboratoire teste l'automatisation du DNSSEC. Ça travaille avec AWS, mais je pense que cela ne posera pas de problème.

Deuxième bloc, une présentation de la part de Régis et Benoit de l'AFNIC. On a travaillé sur différentes technologies, on a abordé cela, les différents concepts de ces technologies, l'importance des communications et de la sécurité. Il y a le blocage des données également, qui a été abordé. SPF est prédominant dans ces technologies concernant les données et ont une belle visualisation des domaines existants et leurs évolutions.

Benoît nous a également donné des exemples amusants des configurations qu'on a vues dans le monde entier. Il y a eu des petits laboratoires pour contrer les différences, donc on a vu comment le SPF fonctionne.

Ensuite il y a eu une présentation de monsieur Limoncelli sur le contrôle du DNS et ses différents outils qui sont configurés. Et d'une manière intéressante, cela a trouvé comme origine certains fichiers et ce contrôle du DNS et ses processus, ont a travaillé sur les différents conflits entre les différents fichiers de la zone. Cela soutient donc les prestataires de service DNS.

Pour rebondir sur ce qu'à fait AFNIC sur le SPF, il y a eu la possibilité de voir comment on pouvait configurer avec DNS contrôle et bâtir différents rapports et assemblées différents fichiers, qu'ils soient plus corrects. On a parlé une nouvelle fois d'automatisation des tâches.

Ensuite, Eberhard a donné un aperçu assez complet, je dois dire, du domaine .NA où on utilise des solutions de registres en tant que bases de données et on utilise également le streaming pour les différentes applications et les différentes solutions de bases de données avec des systèmes d'enregistrements tiers inversés avec des certificats crypto également et des signatures de clés. C'est tout un système assez complexe pour l'analyse et le rapport. Ils utilisent Ubuntu comme système, et ils utilisent le contrôle du DNS également, et ils avaient un manuel de 500 pages pour gérer cela. Et en allant même plus de 500, peut-être 1000 pages, 1500 pages.

Et il va y avoir une nouvelle version qui va être créée et qui sera encore plus complète et qui sera révisée. Et il y a eu une conclusion avec beaucoup d'éléments qui ont été apportés.

Alors le prochain bloc a été présidé par monsieur Smith, du comité de lutte contre l'utilisation malveillante du DNS, pour lutter contrer ces activités. On a parlé de .uk, .us et la salle était pleine, vraiment. Il y a eu beaucoup de personnes qui étaient intéressées qui étaient présentes.

Au début, vous avez dit qu'on utilisait un outil de détection, on a entendu parler de l'évolution du système de vérification manuel au système automatique par la machine, avec une collaboration avec l'université de Lévin. Et cet outil, en lui-même, est limité à .eu, mais on essaye de le rendre disponible à différentes solutions de ccTLD, fournies de cette manière ce service.

Ensuite, des représentants de Nominet ont représenté le système de Genie qui fonctionne sur ChatGPT, et vous pouvez utiliser une langue pour trouver certaines anomalies dans les données.

Et ensuite on a entendu un rapport du registre .us qui a présenté différents blocs d'enregistrements, et la séance s'est terminée sur une séance de questions et réponses avec beaucoup de questions de la part du public.

Et finalement, dans le dernier bloc, qui a commencé par la présentation de Naveed sur l'outil pour explorer le DNSSEC, avec une plateforme qui a été fondée par l'ICANN dont l'objectif était de

scanner 600 millions de domaines en utilisant des outils à source ouverte, comme Kafka et autre. Ils nous ont montré une démonstration de ce projet, et actuellement ils sont en train d'analyser cela et ils vont passer à un autre projet.

La prochaine présentation de Maarten portait sur le fait que ce laboratoire va voir comment remplacer le DNSSEC. C'est quelque dont on a parlé, on a besoin de de deux ans de plus pour régler les problèmes, et ensuite il faudra prendre une décision concernant les changements nécessaires. Il y a plusieurs outils Cascade et autre. Maarten a présenté une liste pour ces logiciels et cela est prévu pour la moitié de l'année prochaine. Donc on a besoin de davantage d'outils et on a besoin d'une grande diversité.

Et la dernière présentation d'aujourd'hui portait sur les risques de collisions des noms de domaines, ou domaines blockchain. On a parlé des recherches faites sur les blockchains, on a parlé d'AFNIC et des recherches faites, et de leurs propres recherches sur des millions d'enregistrements de fournisseurs de blockchain. Ils ont fait des analyses concernant ces systèmes d'intégration DNS et autres.

Et ils ont aussi dit qu'ils faisaient une analyse de données et de l'enregistrement de ce type de données et qu'il faudrait faire davantage de recherche sur ce point-là pour savoir comment ces domaines sont utilisés.

Voilà, j'en ai terminé. J'espère que vous avez apprécié cette journée de Tech Day, que vous avez été intéressé par les

présentations. Je vous souhaite une bonne réunion, et on se croise dans les couloirs ces jours-ci.

LUIS DIÉGO ESPINOZA Bien nous allons applaudir monsieur. Je remercie le public et tous ceux qui ont participé à cette journée technique. Merci.

[FIN DE LA TRANSCRIPTION]