ICANN | GAC
Governmental Advisory Committee

ICANN 72
VIRTUAL ANNUAL GENERAL

Atténuation de l'utilisation malveillante du DNS

Séance 3

Table des matières

Objectifs de la séance

Cette séance vise à poursuivre la prise en compte par le GAC des initiatives de l'organisation ICANN et de la communauté de l'ICANN pour prévenir et atténuer l'utilisation malveillante du DNS. Cela comprend la mise en œuvre des recommandations découlant des révisions de la CCT et de la SSR2, les discussions qui suivent la conclusion du groupe de travail de la GNSO consacré au PDP relatif aux procédures pour des séries ultérieures de nouveaux gTLD, et les récentes propositions du SSAC pour l'établissement d'un facilitateur commun de réponse à des abus. Cette séance sera également l'occasion de poursuivre le débat sur des propositions concrètes possibles du GAC.

Proposition des dirigeants pour la ligne d'action du GAC

1. **Examiner la** résolution **et la** fiche de suivi (22 juillet 2021) **du Conseil d'administration sur les recommandations de la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS (SSR2)** dans son rapport final (25 janvier 2021) sur lequel le GAC avait soumis des commentaires (8 avril 2021)[1].

2. **Examiner les résultats de l'audit de l'ICANN sur la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation de l'utilisation malveillante du DNS** , tel que rapporté dans une annonce et un rapport (24 août 2021).

3. **Examiner la proposition du SSAC pour une** approche interopérable à la gestion de l'utilisation malveillante du DNS (19 mars 2021) y compris la création proposée d'un « facilitateur commun de réponse à des abus » en tant qu'organisation non-gouvernementale à but non-lucratif

[1] Voir aussi le blog de l'organisation ICANN sur la révision de la SSR2 sur les décisions du Conseil d'administration et les prochaines étapes (26 juillet 2021) qui résume les actions du Conseil d'administration.

indépendante qui agirait comme facilitateur pour l'ensemble de l'écosystème du DNS afin de rationaliser les rapports d'abus et de minimiser le nombre de victimes d'abus.

État actuel et développements récents

Discussions de la communauté et mesures concrètes prises à ce jour

- Au cours des récentes réunions de l'ICANN, **les dirigeants du groupe de travail sur la sécurité publique du GAC ont informé** le GAC de la question de l'utilisation malveillante du DNS[2], conformément au Plan de travail 2020-2021 du PSWG et à son objectif stratégique n° 1 visant à renforcer les capacités d'atténuation de l'utilisation malveillante du DNS et de la cybercriminalité.
    - Le GAC a examiné les **mesures mises à la disposition des opérateurs de registre et des bureaux d'enregistrement pour prévenir l'utilisation malveillante du DNS**, en particulier le rôle des politiques d'enregistrement (y compris la vérification d'identité) et des stratégies de tarification comme déterminants clés des niveaux d'abus dans un TLD donné.
    - Le GAC a également examiné des initiatives en cours ou possibles pour traiter plus efficacement l'utilisation malveillante du DNS au niveau du Conseil d'administration de l'ICANN et de l'organisation ICANN[3], y compris des révisions des contrats de l'ICANN avec les opérateurs de registre et les bureaux d'enregistrement, l'application des exigences existantes, la mise en œuvre des recommandations de la révision de la CCT et de la SSR2 pertinentes et des recommandations de politique pour les fournisseurs de service d'anonymisation et d'enregistrement fiduciaire, l'amélioration de l'exactitude des données d'enregistrement et la publication de données plus détaillées des cas d'utilisation malveillante de noms de domaine.

- **Les dirigeants du GAC et du conseil de la GNSO ont discuté des questions spécifiques du GAC** fournies à la GNSO avant chaque réunion de l'ICANN depuis l'ICANN70[4]
    - **Le GAC a demandé à la GNSO des mises à jour sur le travail communautaire qu'elle envisage de mener**, à la lumière des conclusions du PDP sur les séries ultérieures de nouveaux gTLD (qui n'a pas fait de recommandations sur l'atténuation de l'utilisation malveillante du DNS pour les futurs gTLD uniquement), des recommandations de la révision de la SSR2 et des recommandations du SSAC dans son document SAC115.
    - Comme enregistré dans le procès-verbal du GAC del'ICANN70 (p.16) et de l'ICANN71 (p.13), les **dirigeants du conseil de la GNSO ont reconnu l'importance du sujet pour la communauté de l'ICANN** et la longue discussion sur cette question, mais a noté que

[2] Voir les documents de la séance plénière du GAC pendant l'ICANN66, l'ICANN68, l'ICANN69, l'ICANN70 et l'ICANN71

[3] Voir les procès-verbaux de l'ICANN66, le communiqué du GAC et les procès-verbaux de l'ICANN68, le communiqué du GAC et les procès-verbaux de l'ICANN69, le communiqué du GAC et les procès-verbaux de l'ICANN70, et le communiqué du GAC et les procès-verbaux de l'ICANN71.

[4] Voir les messages et les questions au conseil de la GNSO avant l'ICANN70

d'autres travaux exigent une portée appropriée ainsi que le développement **d'une compréhension commune**, en particulier en ce qui concerne la définition de l'utilisation malveillante du DNS et sa compatibilité avec la mission de l'ICANN.

- En ce qui concerne les mesures que la GNSO prévoit de prendre, les dirigeants du conseil de la GNSO ont indiqué que **des consultations avec les parties contractantes** seraient menées et **pourraient conduire à l'identification d'options pour d'autres travaux**. En vertu de la décision du conseil de la GNSO/des décisions et des mesures à prendre (à compter du 23 septembre 2021), « *les prochaines étapes, le cas échéant, sur l'utilisation malveillante du DNS* » restent à déterminer.

- **Mesures et initiatives visant à atténuer l'utilisation malveillante du DNS par les registres et les bureaux d'enregistrement**
  - Le 27 mars 2020, l'organisation ICANN a approuvé la proposition d'amendement du contrat de registre de .COM qui **étend les dispositions contractuelles afin de faciliter la détection et la signalisation de cas d'utilisation malveillante du DNS aux deux tiers de l'espace de noms des gTLD**[5]. En outre, une lettre d'intention contraignante entre l'organisation ICANN et Verisign établit un cadre de coopération pour développer les meilleures pratiques et les nouvelles obligations contractuelles potentielles, ainsi que des mesures visant à mesurer et à atténuer les menaces à la sécurité du DNS.
  - **Dans le contexte de la crise du COVID-19, les parties contractantes et les parties prenantes de la sécurité publique** ont fait rapport[6] sur leur collaboration pour faciliter les rapports, leur révision et leur renvoi à la juridiction compétente à travers l'adoption d'un formulaire normalisé et l'établissement d'un point de contact unique pour les autorités compétentes. Ces efforts ont renforcé les relations de travail établies entre les organismes d'application de la loi et les bureaux d'enregistrement, et s'inspirent de la publication par le **Groupe des représentants des bureaux d'enregistrement** d'un Guide des bureaux d'enregistrement pour le signalement d'abus, dans le cadre de l'ICANN67.
  - Le **Registre d'intérêt public (PIR)**, opérateur de registre de .ORG et de plusieurs nouveaux gTLD, a lancé (17 février 2021) l'**Institut de lutte contre l'utilisation malveillante du DNS**. Cette initiative a été présentée au PSWG du GAC (3 mars 2021). Dans le communiqué de l'ICANN70, le GAC salue la création de l'Institut de lutte contre l'utilisation malveillante du DNS et *« encourage les efforts de la communauté visant à s'attaquer ensemble à la lutte contre l'utilisation malveillante du DNS de manière holistique »*. L'Institut de lutte contre l'utilisation malveillante du DNS a depuis publié une feuille de route (14 juin 2021) et un article (24 août 2021) traitant de l'atténuation des dommages à diverses couches de l'infrastructure Internet.

[5] Ces dispositions incluent la spécification 11 3b qui n'était applicable, jusqu'à présent, qu'aux nouveaux gTLD.

[6] Voir les présentations des parties contractantes avant et pendant la réunion ICANN68 et le document d'information du PSWG au GAC dans le cadre de l'ICANN68.

- **Réponse multidimensionnelle[7] de l'organisation ICANN à l'utilisation malveillante et à la conformité contractuelle**
    - **Le Bureau du directeur de la technologie (OCTO) de l'ICANN et son équipe consacrée à la sécurité, la stabilité et la résilience** (SSR) mènent des recherches et assurent l'expertise de l'ICANN en matière de sécurité du DNS au profit de la communauté. Il est engagé dans des forums de veille en matière de cybermenaces et de réponse aux incidents, et développe des systèmes et des outils pour aider à identifier, analyser et signaler l'utilisation malveillante du DNS[8].
        - En réponse à la crise du COVID-19, l'OCTO a développé l'outil de **signalement et de collecte d'informations sur les menaces à la sécurité des noms de domaine (DNSTICR)** pour aider à identifier les noms de domaine utilisés pour les abus liés au COVID-19 et pour pouvoir partager les données avec les parties pertinentes. Le GAC a été informé de cette question avant l'ICANN68 (12 juin 2020) et les membres ont été invités à contribuer à la diversité linguistique de l'outil.
        - Grâce à sa **plateforme de signalement des cas d'utilisation malveillante des noms de domaine (DAAR)**, l'ICANN rend compte tous les mois, depuis janvier 2018, de l'enregistrement de noms de domaine et des menaces à la sécurité observées dans le DNS[9].
        - L'OCTO de l'ICANN soutient le **Groupe d'étude technique chargé de l'initiative de facilitation de la sécurité du DNS**, récemment créé en mai 2020 dans le cadre de la mise en œuvre du plan stratégique pour les exercices fiscaux 2021 à 2025, dans le but de *« réfléchir à ce que l'ICANN peut et devrait faire pour augmenter le niveau de collaboration et d'engagement avec les parties prenantes de l'écosystème du DNS afin d'améliorer le profil de sécurité du DNS »*. Un rapport sur l'état d'avancement a été présenté lors du 4e Symposium sur le DNS (24 mai 2021) et devrait être présenté avant l'ICANN72.

Le PDG de l'ICANN a publié un billet de blog le 20 avril 2020 détaillant la réponse multidimensionnelle de l'organisation ICANN à l'utilisation malveillante du DNS.

Lors d'un appel du GAC portant sur des questions liées à l'utilisation malveillante du DNS (24 février 2021), l'organisation ICANN a fait le point sur les activités liées à l'utilisation malveillante du DNS de l'OCTO, dont une discussion sur la définition des menaces à la sécurité du DNS et de l'utilisation malveillante du DNS, les obligations des parties contractantes, le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR), les informations relatives aux menaces à la sécurité des noms de domaine, l'outil de signalement et de collecte d'information sur des menaces à la sécurité des noms de domaine (DNSTICR), la nouvelle initiative visant à élaborer des normes pour le partage de connaissances et l'instauration pour la sécurité du DNS et du nommage (KINDNS), et une révision des efforts de l'OCTO dans le domaine de la formation et du renforcement des capacités à travers le monde.

[9] Plusieurs parties prenantes et initiatives de l'ICANN ont commenté les limites du DAAR, en particulier une lettre du M3AAWG à l'organisation ICANN (5 avril 2019) et le rapport préliminaire de l'équipe de révision SSR2 (24 janvier 2020). Le groupe des représentants des opérateurs de registre, qui avait également exprimé des préoccupations, a formulé des recommandations dans une correspondance adressée au CTO de l'ICANN (9 septembre 2020).

- Pour ce qui est de **l'application de la conformité contractuelle,** dans son billet de blog (20 avril 2020), le PDG de l'ICANN a rappelé ce qui suit : « *Le département de l'ICANN chargé de la conformité contractuelle de l'ICANN veille au respect des obligations établies dans les politiques et les contrats de l'ICANN, en particulier le contrat de registre (RA) et le contrat d'accréditation des bureaux d'enregistrement (RAA). Ce département travaille également de manière étroite avec l'OCTO à identifier des menaces à la sécurité du DNS [...] et à les relier aux parties contractantes concernées. Le département de l'ICANN chargé de la conformité contractuelle se sert des données collectées pendant les audits [...] pour évaluer si les opérateurs de registre et les bureaux d'enregistrement se conforment à leurs obligations en matière d'atténuation des menaces à la sécurité du DNS. En dehors de ces audits, le département de l'ICANN chargé de la conformité contractuelle utilisera les données collectées par l'OCTO et d'autres pour contacter de manière proactive des registres et des bureaux d'enregistrement qui affichent un nombre disproportionné de menaces à la sécurité du DNS. En cas d'échec du dialogue constructif, le département de l'ICANN chargé de la conformité contractuelle n'hésitera pas à faire exécuter les contrats de tous ceux qui refuseraient de se conformer à leurs obligations en matière de menaces à la sécurité du DNS ».*
  Le billet de blog a également fourni un aperçu du volume de plaintes, des ressources allouées à leur traitement et des statistiques sur la résolution de ces plaintes[10].
- À la suite d'un **audit de conformité contractuelle** préalable de l'opérateur de registre axé sur l'utilisation malveillante de l'infrastructure du DNS qui s'est achevé en juin 2019[11] , l'ICANN a présenté (le 24 août 2021) les résultats de l'audit sur **la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation des risques liés à la sécurité du DNS** :
  - 126 bureaux d'enregistrement audités (gérant plus de 90 % de tous les domaines enregistrés dans les gTLD)
  - 111 bureaux d'enregistrement ne satisfaisant pas entièrement aux exigences relatives à la réception et au traitement des signalements d'utilisation malveillante du DNS (sections 3.18.1 à 3.18.3 du RAA).
  - 92 bureaux d'enregistrement ont pris des mesures pour devenir entièrement conformes et 19 mettent en œuvre des changements
- L'organisation ICANN a présenté (22 juillet 2021) son programme d'atténuation des menaces à la sécurité du DNS , qui vise à fournir une visibilité et une clarté sur les diverses initiatives et projets liés aux menaces à la sécurité du DNS et permet la formation et l'exécution d'une stratégie centralisée.

[10] Des rapports réguliers sur la conformité contractuelle sont disponibles à l'adresse suivante : https://www.icann.org/resources/compliance-reporting-performance

[11] Voir le blog de l'ICANN « Conformité contractuelle :Traiter les cas d'utilisation malveillante de l'infrastructure du DNS (système des noms de domaine) » (8 novembre 2018) et le « Rapport d'audit du département chargé de la conformité contractuelle sur la réponse des opérateurs de registre aux menaces à la sécurité du DNS » (17 septembre 2019)

Recommandations de la communauté pour les travaux futurs

- **Recommandations issues de la révision SSR2**
  - L'équipe de révision SSR2 a présenté un rapport préliminaire (24 janvier 2020) qui met l'accent sur les mesures visant à prévenir et à atténuer l'utilisation malveillante du DNS. Le commentaire du GAC (3 avril 2020) soutenait bon nombre des recommandations, y compris celles portant sur l'amélioration du système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) et le renforcement des mécanismes de conformité.
  - Le rapport final (25 janvier 2021) a été examiné par le GAC lors de l'ICANN70 en vue de la soumission finale des commentaires du GAC (8 avril 2021) dans le cadre de la procédure de consultation publique.
  - Le Conseil d'administration de l'ICANN a pris des mesures (22 juillet 2021) concernant les 63 recommandations finales de l'équipe de révision (25 janvier 2021). Un blog de l'organisation ICANN associé a résumé les types d'actions entreprises comme suit :
    - 13 recommandations ont été approuvées (en attendant la planification de leur mise en œuvre),
    - 16 recommandations ont été rejetées (y compris 6 qui n'ont pas pu être entièrement approuvées),
    - 34 recommandations sont en attente d'informations et d'analyses complémentaires.
- **L'équipe de travail consacrée à l'utilisation malveillante du DNS du Comité consultatif sur la sécurité et la stabilité (SSAC)** a publié son rapport SAC115 (19 mars 2021) qui propose une approche interopérable pour la gestion de l'utilisation malveillante du DNS.
  - Dans ce rapport, le **SSAC propose un cadre général de bonnes pratiques et de processus** visant à optimiser le signalement des cas d'utilisation malveillante du DNS et des cas d'abus sur Internet en général, prévoyant notamment : un responsable principal pour le règlement de litiges relatifs à l'utilisation malveillante, des normes en matière de preuve, des mécanismes d'intervention progressive, un calendrier d'action raisonnable et la mise à disposition d'informations de contact de qualité.
  - **La principale proposition** que le SSAC recommande de faire examiner et peaufiner par la communauté de l'ICANN en lien avec l'ensemble de la communauté chargée des infrastructures du DNS **est la création d'un « facilitateur de réponse commune aux abus »** sous la forme d'une organisation non gouvernementale à but non lucratif pleinement indépendante qui ferait office de facilitateur pour l'ensemble de l'écosystème du DNS, qui comprendrait les parties contractantes de l'ICANN, les fournisseurs d'hébergement, les fournisseurs de services Internet (FSI) et les réseaux de diffusion de contenu (CDN), afin d'optimiser le signalement des cas d'utilisation malveillante et de minimiser le nombre de victimes d'abus.

Principaux documents de référence :

- Rapport final de la révision de la SSR2 (25 janvier 2021) et fiche de suivi des mesures prises par le Conseil d'administration (22 juillet 2021)
- Annonce et rapport de l'ICANN (24 août 2021) sur l'audit sur la conformité des bureaux d'enregistrement aux obligations en matière d'atténuation des risques liés à la sécurité du DNS.
- Le Rapport SAC115 (19 mars 2021) du SSAC, qui propose une approche interopérable pour traiter la gestion de l'utilisation malveillante du DNS

Informations complémentaires

Document de contexte de la politique du GAC sur l'atténuation de l'utilisation malveillante du DNS
https://gac.icann.org/briefing-materials/public/gac-policy-background-dns-abuse-mitigation.pdf

Gestion des documents

Titre	Document d'information du GAC sur l'ICANN71 - Séance 3 - Utilisation malveillante du DNS
Distribution	Membres du GAC (avant la réunion) et public en général (après la réunion)
Date de distribution	Version 1 : 22 sept. 2021