ICANN | GAC

Governmental Advisory Committee

Distribution	Publique
Date	18 septembre 2019

Déclaration du GAC sur l'utilisation malveillante du DNS

Le Comité consultatif gouvernemental (GAC) de l'ICANN attend avec impatience la prochaine discussion intercommunautaire sur l'utilisation malveillante du DNS lors de l'ICANN66 et il est sensible à la lettre ouverte datée du 19 août 2019 du groupe des représentants des opérateurs de registres à la communauté sur ce sujet.

Protéger le public des menaces à la sécurité et de l'utilisation malveillante du DNS est une question de politique publique importante. Le GAC a émis un avis, a apporté ses conseils et commentaires, a organisé des discussions intercommunautaires, et a prôné le renforcement des dispositions contractuelles afin de protéger le public.[1] Nos observations actuelles apporteront davantage de contexte sur ce sujet en discutant : 1) des raisons pour lesquelles l'utilisation malveillante du DNS est un sujet essentiel ; 2) des définitions existantes et des obligations contractuelles concernant l'utilisation malveillante du DNS ; et 3) des conclusions et recommandations de l'équipe de révision de la concurrence, la confiance et le choix du consommateur sur l'utilisation malveillante du DNS. Grâce à ces discussions nous espérons poser les bases d'une discussion intercommunautaire productive et informée, à Montréal.

Pourquoi l'utilisation malveillante du DNS est un sujet essentiel

D'année en année, le coût global de la cybercriminalité augmente. On l'estime à 600 milliards de dollars en 2018.[2] Les cybercriminels exploitent et utilisent avec malveillance le DNS pour accomplir leurs tâches [3] et le courrier électronique est de loin le vecteur le plus courant d'un compromis initial [4] avec une forte augmentation de l'hameçonnage contre les consommateurs.[5]

Si le public doit faire confiance et s'appuyer sur Internet pour ses communications et transactions, ceux qui sont chargés de gérer l'infrastructure du DNS doivent prendre des mesures pour garantir que cette ressource publique est en sécurité.

---

1 Le GAC a apporté ce commentaire de manière indépendante et par le biais du groupe de travail sur la sécurité publique. Voir p.ex., ce qui suit : Communiqués du GAC : ICANN46 Beijing; ICANN 53 Buenos Aires, ICANN54 Dublin; et ICANN57 Hyderabad; présentations de la communauté de l'ICANN concernant l'utilisation malveillante du DNS lors de l'ICANN57, 58, et 60; et recommandations de 2009 concernant l'application de la loi (approuvées par le GAC lors de l'ICANN38).

2 McAfee Economic Impact of Cybercrime – No Slowing Down (McAfee L'impact économique des cybercrimes - aucun ralentissement) disponible à l'adresse : https://www.csis.org/analysis/economic-impact-cybercrime; Accenture 2019 Cost of Cybercrime (Accenture 2019 Le coût des cybercrimes), disponible à l'adressehttps://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

3 *Voir p.ex.,* Symantec Internet Threat Security Report (Symantec Rapport sur les menaces à la sécurité de l'Internet) (Fev 2019) disponible à l'adresse : https://www.symantec.com/security-center/threat-report.

4 2019 Data Breach Investigations Report (Rapport d'enquêtes 2019 sur la violation des données) de Verizon disponible sur : https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations- report.pdf

5 Akamai's 2019 State of the Internet (Rapport 2019 de Akamaï sur l'état des lieux de l'internet) disponible à l'adresse : https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial- services-attack-economy-report-2019.pdf

Les lois récentes en matière de vie privée, dont le Règlement général sur la protection des données (RGPD) de l'Union-Européenne, ont limité l'accessibilité au public des informations concernant les propriétaires des noms de domaine, créant des difficultés pour les professionnels chargés de l'application de la loi et de la cybersécurité qui ont pour mission de combattre les menaces liées à la sécurité de l'Internet.[6]

Les révisions récentes et actuelles de l'ICANN, demandées en vertu des statuts constitutifs ont mis en avant l'importance :

- de **l'efficacité des efforts en matière de sécurité pour traiter les problématiques actuelles et éventuelles ainsi que les menaces liées à la sécurité et stabilité du DNS**, et la mesure dans laquelle **les efforts liés à la sécurité sont suffisamment importants pour répondre aux défis** et menaces futurs ;[7]
- de la **protection du consommateur**, de la sécurité, stabilité et résilience, des questions de **malveillances**, des inquiétudes vis-à-vis de la souveraineté, et de la protection des droits avant, ou pendant, l'autorisation d'augmentation du nombre de nouveaux domaines de premier niveau ;[8]
- d'**améliorer l'exactitude et l'accès aux données d'enregistrement des domaines génériques de premier niveau**, et d'envisager la mise en place de sauvegardes pour les protéger ;[9]
- de l'**efficacité** du **service d'annuaire des données d'enregistrement de gTLD** en vigueur à ce moment et savoir **si sa mise en œuvre répond aux besoins légitimes des agences chargées de l'application de la loi, promeut la confiance du consommateur** et sauvegarde les données des titulaires de noms de domaine[10] [emphase ajoutée]

De plus, l'ICANN étudie le profil d'une deuxième série de gTLD qui donne l'occasion d'inclure dans les contrats des mesures incitatives pour adopter de meilleures pratiques permettant de réduire ces utilisations malveillantes et augmenter le coût des activités des acteurs criminels.

Par conséquent, c'est le bon moment pour étudier ces questions et envisager la meilleure voie à suivre pour soutenir l'engagement de l'ICANN de préserver et **améliorer** la gestion du DNS, dont notamment « la stabilité opérationnelle, la fiabilité, la sécurité, l'interopérabilité mondiale, la résilience, et l'ouverture du DNS et de l'Internet. »[11]
À cet égard, les gouvernements et les autorités publiques sont les mieux placés pour apporter des commentaires.[12]

6 Voir p.ex., Enquête de l'ICANN sur le RGPD et les utilisateurs WHOIS réalisée par un groupe de travail anti-hameçonnage et un groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles, disponible à l'adresse :https://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.html

7, Statuts constitutifs de l'ICANN, §4.6 (c), Révision sur la sécurité, stabilité et résilience.

8 Statuts constitutifs de l'ICANN, §4.6 (d), Révision de la concurrence, la confiance et le choix du consommateur

9 Statuts constitutifs de l'ICANN, §4.6 (e), Révision du service d'annuaire des données d'enregistrement.

10 *Id.*

11 Statuts constitutifs de l'ICANN §1.2(a) Engagements

12 En effet, reconnaître le rôle essentiel que les gouvernements et autorités publiques jouent lorsque surviennent des problématiques relatives à des questions de politique publique, est une des valeurs fondamentales de l'ICANN. Statuts constitutifs de l'ICANN, §1.2(b) Valeurs fondamentales.

Définitions existantes de l'utilisation malveillante du DNS et obligations contractuelles de l'ICANN

L'équipe de révision de la concurrence, confiance et choix du consommateur (CCT) qui est composée de parties prenantes provenant de l'ensemble de la communauté de l'ICANN, a observé les définitions existantes de l'utilisation malveillante du DNS au sein de la communauté de l'ICANN alors qu'elle cherchait à examiner l'utilisation malveillante du DNS au sein des nouveaux gTLD par rapport aux gTLD historiques et à savoir si les sauvegardes existantes étaient suffisantes.[13] Il convient de noter que les conclusions de la communauté de l'ICANN ont démontré « qu'un consensus existe sur ce qui constitue un abus en matière de sécurité du DNS ou un abus en matière de sécurité de l'infrastructure du DNS, » **l'équipe de révision CCT utilise l'expression utilisation malveillante du DNS pour faire référence à « des activités volontairement trompeuses, sournoises ou non sollicitées qui utilisent activement le DNS et/ou les procédures d'enregistrement des noms de domaine »**[14] Le rapport CCT a utilisé l'expression « utilisation malveillante du DNS » pour faire référence à des formes plus techniques de l'activité malveillante telles que : logiciel malveillant, hameçonnage et réseau zombie, ainsi que le spam lorsqu'il est utilisé comme une méthode de diffusion pour d'autres formes d'abus.[15]

Ces définitions sont conformes aux contrats standards de l'ICANN pour les registres et bureaux d'enregistrement. Le contrat de registre de base imposait aux opérateurs de registre de nouveaux gTLD d'inclure dans leur contrat registre-bureau d'enregistrement des dispositions interdisant aux titulaires de nom de domaine :

> « la diffusion de programmes malveillants, l'exploitation abusive de réseaux zombies, le hameçonnage, la piraterie, la violation de marques ou de propriété intellectuelle, les pratiques frauduleuses ou nuisibles, les contrefaçons ou autres activités contraires aux lois applicables, et prévoyant (conformément aux lois applicables et aux procédures y afférentes) des sanctions pour ce type d'activités, y compris la suspension du nom de domaine ».[16]

En outre, les opérateurs de registre doivent « procéder périodiquement à une analyse technique afin d'évaluer si les domaines du TLD sont utilisés de façon à perpétrer des menaces à la sécurité **comme** le dévoiement, l'hameçonnage, les programmes malveillants et les réseaux zombies ».[17] [emphase ajoutée]. Nous notons que cette liste est donnée à titre indicatif plutôt qu'à titre exhaustif.

---

[13] Voir rapport final de la CCT (18 sept 2018) aux pages 88-109. Pour en savoir plus sur la manière dont l'utilisation malveillante a été définie par la communauté de l'ICANN, voir le rapport final du groupe de travail en charge des politiques (23 mai 2010) : https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf

[14] Rapport final de la CCT à la page 88 et accompagnant les conclusions. Voir également la page 3 du « rapport révisé (2016) : sauvegardes du programme des nouveaux gTLD face à l'utilisation malveillante du DNS ».

[15] Rapport final de la CCT à la page 8.

[16] Contrat de registre de l'ICANN, spécification 11, 3(a).

[17] Contrat de registre de l'ICANN, spécification 11, 3(b). Cette disposition a été le thème répété des questions, inquiétudes et avis du GAC qui sont apparus car la mise en œuvre par l'ICANN de cette sauvegarde tout en demandant aux registres de surveiller les menaces à la sécurité, n'obligeait pas les opérateurs de registre à agir en réponse aux menaces à la sécurité. *Voir* Singapour (2014), Los Angeles, Londres. Le communiqué de Beijing du GAC comportait, non seulement un devoir de surveillance des menaces à la sécurité, mais aussi un devoir de réponse dans le cas

Pour compléter les dispositions du registre, le contrat standard de l'ICANN pour les bureaux d'enregistrement exige que ces derniers « enquêtent rapidement et répondent de manière appropriée à tout signalement de malveillance. »[18] Ensemble, ces sources développées au sein de la communauté multipartite de l'ICANN constituent une compréhension fondamentale commune de ce qui compose une utilisation malveillante du DNS.

L'équipe de révision CCT déclare que les utilisations malveillantes du DNS se concentrent autour de certains registres et bureaux d'enregistrement et a donc développé des recommandations

L'équipe de révision CCT a observé que les noms de domaine sont un composant majeur de la cybercriminalité, utilisés pour la distribution de logiciels malveillants et pour la commande et le contrôle de réseaux zombies, et ont observé que les campagnes de spam sont souvent associées à de l'hameçonnage et d'autres cybercrimes.[19] L'équipe de révision a notamment souligné que

> même si les contrats standards de l'ICANN pour les registres et bureaux d'enregistrement imposent une utilisation conforme de sauvegardes spécifiques, les efforts pour lutter contre l'utilisation malveillante de noms de domaine varient considérablement selon les parties contractantes. Certaines entités n'agissent pas avant la réception d'une plainte. En revanche, d'autres bureaux d'enregistrement prennent des mesures proactives comme la vérification des informations d'identification d'un titulaire de nom de domaine, le blocage de chaînes de noms de domaine similaires à des cibles d'hameçonnage connues, et l'examen des revendeurs de noms de domaine. Les revendeurs de noms de domaine ne sont pas des parties contractantes de l'ICANN et ne sont donc pas directement soumis aux obligations contractuelles de l'organisme de l'ICANN chargé de l'application de la loi.[20]

Afin de mieux comprendre l'efficacité des sauvegardes des nouveaux gTLD, l'équipe de révision CCT a demandé une étude pour analyser les taux de répartition entre le spam, l'hameçonnage et les logiciels malveillants au sein des gTLD au niveau mondial de 2014 à 2016, en distinguant les nouveaux gTLD des gTLD historiques et a publié le rapport en découlant.[21] L'étude sur l'utilisation malveillante du DNS a clairement montré qu'il y a des problèmes de malveillance importants au sein du DNS. Concernant le programme des nouveaux gTLD, l'étude montre que plus de 50 % des enregistrements dans certains nouveaux gTLD ont été malveillants.[22] D'autres faits ont été mis en avant par l'étude :

- les nouveaux gTLD sont devenus une cible croissante pour les personnes malveillantes ;
- les gTLD historiques ont une plus grande concentration de domaines compromis alors que les criminels choisissent souvent d'enregistrer par malveillance des noms de domaine utilisant un des nouveaux gTLD ;
- les opérateurs de registre qui pratiquent une concurrence des prix ont le plus grand nombre de nouveaux gTLD victimes de malveillances ;
- les taux d'hameçonnage et de logiciels malveillants concernant les nouveaux gTLD convergent avec les taux de gTLD historiques au fil du temps ;
- cinq nouveaux gTLD ayant le taux le plus élevé de domaines utilisés dans les attaques d'hameçonnage selon la liste noire du groupe de travail anti-hameçonnage contenaient 58,7 % de l'ensemble des domaines sur liste noire au sein des nouveaux gTLD ;

---

[18] Contrat de bureau d'enregistrement de l'ICANN § 3.18.
[19] Rapport finale de l'équipe de révision final de la CCT à la page 93.
[20] Rapport finale de l'équipe de révision final de la CCT à la page 93.
[21] *Voir*https://www.icann.org/news/announcement-2017-08-09-en
[22] Analyse statistique de l'utilisation malveillante du DNS dans le rapport final sur les gTLD (9 août 2017) ; https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

- Les nouveaux gTLD ont connu un pourcentage plus élevé de spam au dernier trimestre 2016 par rapport aux gTLD historiques (10 fois plus élevé que les gTLD historiques) ;
- Les noms de domaine enregistrés à des fins malveillantes contenaient souvent des chaînes en lien avec les termes de marques déposées
- Le recensement des malveillances correspond principalement à des exigences strictes d'enregistrement : autrement dit, les personnes malveillantes préfèrent enregistrer des domaines au sein des nouveaux gTLD standards qui sont en général ouverts à un enregistrement public, plutôt qu'à des nouveaux gTLD communautaires pour lesquels les registres peuvent imposer des restrictions quant aux entités qui peuvent enregistrer ces noms de domaine.

L'équipe de révision CCT a conclu que les facteurs comme les restrictions d'enregistrement, le prix et les pratiques spécifiques à un bureau d'enregistrement sont plus susceptibles d'avoir un impact sur le taux de malveillance.[23] Par conséquent, l'équipe de révision CCT a recommandé que :

- l'organisation de l'ICANN négocie des amendements aux contrats de registre existants, ou dans les négociations des nouveaux contrats de registre liés aux futures séries de nouveaux gTLD, **afin d'inclure des dispositions visant à apporter des incitations, y compris des incitations financières aux registres et en particulier aux registres ouverts, afin d'adopter des mesures anti-malveillance proactives**.[emphase ajoutée] ;
- l'organisation de l'ICANN négocie des amendements au contrat d'accréditation de bureau d'enregistrement et aux contrats de registre pour inclure des dispositions visant à empêcher une utilisation systématique de registres ou bureaux d'enregistrement spécifiques pour les menaces à la sécurité du DNS. L'ICANN devrait, en particulier, établir des seuils de malveillance à partir desquels des enquêtes de conformité sont systématiquement déclenchées, avec un seuil plus important à partir duquel les bureaux d'enregistrement et registres sont présumés être en défaut vis-à-vis de leurs contrats ;
- Une étude plus approfondie a été menée sur la relation entre des opérateurs de registre, des bureaux d'enregistrement spécifiques et les menaces à la sécurité du DNS en demandant une collecte continue de données, y compris mais sans s'y limiter, des initiatives de signalement des cas d'utilisations malveillantes des noms de domaine (DAAR). Pour des questions de transparence, ces informations seront régulièrement publiées, idéalement tous les trimestres et au moins une fois par an, afin de permettre l'identification des registres et bureaux d'enregistrement qui exigent un examen et une enquête plus approfondis et des mesures éventuelles prises par l'organisation de l'ICANN. En identifiant des phénomènes de malveillance, l'ICANN devrait mettre en place un plan d'action pour répondre à ces études, remédier aux problèmes identifiés, et définir une future collecte de données ; et
- L'ICANN devrait collecter des données et diffuser la chaîne des parties responsables de l'ensemble des enregistrements de noms de domaine gTLD.

[23] Rapport final de la CCT à la page 94 citant l'étude sur l'utilisation malveillante du DNS aux pages 24-25.

Meilleures pratiques des registres ccTLD

Ces dernières années, un nombre croissant de registres ccTLD ont adopté des mesures anti-abus proactives pour répondre aux crimes contre le DNS et ils ont gardé leur environnement à l'abri des malveillances et ont repoussé les personnes malveillantes en rendant leurs noms de domaine aussi peu attrayants que possible. Ces mesures vont de méthodes d'authentification renforcées, comme les vérifications de l'identité, [24] à l'utilisation de modèles de prédiction de la fraude basés sur les données qui combinent un enregistrement des données et des indicateurs d'infrastructure pour identifier et prévoir les enregistrements de domaine réalisés à des fins préjudiciables. [25] Ces meilleures pratiques prouvées devraient être mises en œuvre par les registres gTLD et bureaux d'enregistrement.

Conclusion

Cette communauté bénéficie d'une position unique pour évaluer et choisir les politiques qui devraient être prises afin de protéger le public de l'utilisation malveillante du DNS. Nous sommes d'accord avec le groupe des représentants des opérateurs de registres pour dire que le succès de leur produit (et celui du DNS) dépend de leur capacité à proposer un produit fiable auquel les utilisateurs pourront avoir confiance. Pour lutter plus efficacement contre l'utilisation malveillante du DNS et favoriser un DNS plus fiable, nous encourageons la communauté à envisager sérieusement d'adopter les recommandations décrites ci-dessus car elles représentent des mesures réalisables pouvant et *devant* être prises pour répondre au problème de l'utilisation malveillante du DNS. Le GAC attend avec impatience de collaborer avec d'autres groupes communautaires sur ce sujet lors de l'ICANN66 à Montréal.

[24] Voir p.ex., Séance de l'ICANN64 sur les leçons apprises : Comment .DK a réduit avec succès les domaines malveillants et https://www.dk-hostmaster.dk/en/news/mandatory- identification-nemid et https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult

[25] Voir https://eurid.eu/en/news/identification-of-malicious-dns/