



Sauvegardes du programme des nouveaux gTLD contre l'utilisation malveillante du DNS

Opérations et politiques de recherche de l'ICANN | Mars 2016

Table des matières

<u>INTRODUCTION</u>	1
<u>UTILISATION MALVEILLANTE DU DNS : TERMINOLOGIE A RETENIR</u>	4
GROUPE DE TRAVAIL SUR LES POLITIQUES RELATIVES AUX ENREGISTREMENTS FRAUDULEUX	6
<u>UTILISATION MALVEILLANTE DU DNS : STATISTIQUES CLES ET PRINCIPALES TENDANCES</u>	12
UTILISATION MALVEILLANTE DU DNS POUR LES NOUVEAUX GTLD	14
ÉTUDE DE CAS SUR L'UTILISATION MALVEILLANTE DU DNS : L'HAMEÇONNAGE DES NOUVEAUX GTLD	16
<u>LES NEUF SAUVEGARDES</u>	18
QUESTION : COMMENT S'ASSURER QUE DES PERSONNES MALVEILLANTES N'EXPLOITENT PAS DE REGISTRES ?	18
SAUVEGARDE : VERIFICATION DES OPERATEURS DE REGISTRE	19
QUESTION : COMMENT GARANTIR L'INTEGRITE ET L'UTILITE DES INFORMATIONS DE REGISTRE ?	21
SAUVEGARDE : FOURNITURE D'UN PLAN ETABLI POUR LE DEPLOIEMENT DES DNSSEC	21
SAUVEGARDE : INTERDICTION DES CARACTERES GENERIQUES	23
SAUVEGARDE : SUPPRESSION DES ENREGISTREMENTS ORPHELINS DE TYPE GLUE	26
QUESTION : COMMENT VEILLER A CE QUE LES INITIATIVES MISES EN PLACE SE CONCENTRENT DAVANTAGE SUR LA LUTTE CONTRE LES UTILISATIONS MALVEILLANTES IDENTIFIEES ?	28
SAUVEGARDE : EXIGENCE CONCERNANT LES ENREGISTREMENTS WHOIS DETAILLE	28
SAUVEGARDE : CENTRALISATION DE L'ACCES AUX FICHIERS DE ZONE	30
SAUVEGARDE : DOCUMENTATION DES POINTS DE CONTACTS ET DES PROCEDURES POUR LE SIGNALEMENT D'ABUS AU NIVEAU DU REGISTRE	32
SAUVEGARDE : PARTICIPATION A UN PROCESSUS DE REQUETE DE SECURITE DE REGISTRE ACCELEREE (ESRS)	33
QUESTION : COMMENT FOURNIR UN CADRE DE CONTROLE AMELIORE POUR LES TLD AVEC UN POTENTIEL INTRINSEQUE DE COMPORTEMENTS MALVEILLANTS ?	34
SAUVEGARDE : CREER UN PROJET DE CADRE POUR UN PROGRAMME DE VERIFICATION DES ZONES DE HAUTE SECURITE	34
<u>PROPOSITION ET MODELES DE RECHERCHE</u>	36
POSSIBLE CADRE QUALITATIF POUR TESTER L'EFFICACITE DES SAUVEGARDES	37
PLAN DE REGISTRE : QUESTIONS ET CONSIDERATIONS CLES	37
MODELES CAUSAUX ET HYPOTHESES	39
<u>ANNEXE : ÉTUDE SUR LES ACTIVITES LIEES AUX UTILISATIONS MALVEILLANTES AU SEIN DE L'ICANN</u>	43

Introduction

Conformément à la section 9.3 de l'[Affirmation d'engagements](#) (AoC) qui vise à encourager la concurrence, le choix du consommateur et la confiance du consommateur dans le système des noms de domaine (DNS), le présent rapport a pour but de faciliter les travaux de l'équipe de révision sur la concurrence, la confiance et le choix du consommateur (CCT-RT). Pour ce faire, il :

- Fournira un aperçu de la situation de l'utilisation malveillante du DNS suite au lancement du programme des nouveaux domaines génériques de premier niveau (gTLD) en janvier 2012.
- Débattrà des options permettant de mesurer l'efficacité des neuf sauvegardes mises en place afin d'atténuer l'utilisation malveillante des nouveaux gTLD.
- Proposera un modèle de recherche afin de faciliter l'évaluation de l'efficacité des neuf sauvegardes quant à l'atténuation de l'utilisation malveillante des nouveaux gTLD.

L'[AoC](#) prévoit ce qui suit :

L'ICANN organisera une révision qui permettra d'évaluer dans quelle mesure le... développement des gTLD encourage la concurrence, la confiance et le choix des consommateurs, ainsi que l'efficacité des... **sauvegardes mises en place pour atténuer les problèmes liés au... développement...** [gras rajouté]. Les révisions seront effectuées par les membres de la communauté de bénévoles et l'équipe de révision sera composée et publiée à des fins de consultation publique. Les recommandations découlant des révisions sera transmises au Conseil d'administration et publiées à des fins de consultation publique. Le Conseil d'administration prendra une décision dans les six mois suivant la réception des recommandations.

En vue du développement potentiel du DNS, l'ICANN a demandé l'avis d'unités constitutives spécialisées quant à l'éventuelle augmentation des activités malveillantes, frauduleuses et criminelles dans le cadre d'un DNS étendu et afin de formuler des recommandations visant à **atténuer à l'avance** l'effet de ces activités via un certain nombre de **sauvegardes**.¹ L'initiative consistant à identifier les étapes visant à atténuer une éventuelle utilisation malveillante a débuté en posant quatre questions à des experts issus de différents groupes dont le groupe de travail anti-hameçonnage (APWG), le groupe de sécurité Internet du registre (RISG), le Comité consultatif sur la sécurité et la stabilité (SSAC), les équipes de réponse aux urgences

¹ "Mitigating Malicious Conduct", ICANN, Mémoire explicatif du programme des nouveaux gTLD, 3 octobre 2009, <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

informatiques (CERT) et les membres des communautés bancaire, financière et de la sécurité d'Internet. Ces questions sont les suivantes :

- 1) Comment s'assurer que des personnes malveillantes n'exploitent pas de registres ?
- 2) Comment garantir l'intégrité et l'utilité des informations de registre ?
- 3) Comment veiller à ce que les initiatives mises en place se concentrent davantage sur la lutte contre les utilisations malveillantes identifiées ?
- 4) Comment fournir un cadre de contrôle amélioré pour les TLD avec un potentiel intrinsèque de comportements malveillants ?

Après de larges consultations, les groupes d'experts ont dégagé les **recommandations** suivantes pour chaque domaine thématique :

Question	Recommandation(s)
1) Comment s'assurer que des personnes malveillantes n'exploitent pas de registres ?	1) Procéder à une vérification des antécédents des opérateurs de registre afin de réduire le risque qu'un opérateur de registre ait été condamné pour comportement criminel, malveillant et/ou de mauvaise foi.
2) Comment garantir l'intégrité et l'utilité des informations de registre ?	2) Exiger le déploiement des extensions de sécurité du système des noms de domaine (DNSSEC) pour tous les nouveaux registres afin de minimiser le risque d'usurpation des enregistrements DNS. 3) Interdire les « caractères génériques » afin d'empêcher la redirection du DNS et la synthétisation des réponses du DNS susceptibles de se produire lors d'une connexion à des sites malveillants. 4) Encourager la suppression des enregistrements orphelins de type glue afin de minimiser l'utilisation de ces restes de domaines préalablement supprimés des enregistrements de registre en tant qu'entrées de serveur de nom « sûres » dans le fichier de zone de TLD que des personnes malveillantes peuvent exploiter.

3) Comment veiller à ce que les initiatives mises en place se concentrent davantage sur la lutte contre les utilisations malveillantes identifiées ?

- 5) **Exiger des enregistrements WHOIS détaillé** afin d'encourager la disponibilité et l'exhaustivité des données WHOIS.
- 6) **Centraliser l'accès au fichier de zone** afin de créer un moyen plus efficace d'obtention de mises à jour sur de nouveaux domaines au fur et à mesure qu'ils sont créés au sein de chaque zone TLD.
- 7) **Documenter les contacts et politiques d'utilisation malveillante au niveau du registre et du bureau d'enregistrement** afin de fournir un correspondant unique chargé de traiter les plaintes pour abus.
- 8) **Prévoir un processus de demande accélérée de sécurité de registre** afin de traiter les menaces en termes de sécurité impliquant la prise de mesures immédiates par l'opérateur de registre et une réponse accélérée de l'ICANN.

4) Comment fournir un cadre de contrôle amélioré pour les TLD avec un potentiel intrinsèque de comportements malveillants ?

- 9) **Créer un projet de cadre pour un programme de vérification des zones de haute sécurité** afin de fixer un ensemble de critères pour assurer la confiance dans les TLD présentant un risque plus élevé de ciblage des personnes malveillantes, par exemple les TLD relevant du domaine bancaire et pharmaceutique, via des contrôles améliorés en termes d'exploitation et de sécurité.

La mesure de l'efficacité de ces sauvegardes constitue l'un des principaux objectifs des travaux de la CCT-RT. Afin de faciliter ces travaux, le présent rapport procède à un examen approfondi de chacune de ces sauvegardes, propose des moyens permettant, le cas échéant, de mesurer leur efficacité et présente un modèle de recherche capable d'analyser leur efficacité de manière rigoureuse et globale. Il convient de noter que le présent rapport est censé *aider* la CCT-RT. Il est censé proposer d'éventuelles méthodes et susciter des discussions au sein de l'équipe concernant la meilleure approche à adopter pour l'étude des utilisations malveillantes du DNS et des

sauvegardes mises en place afin d'atténuer ces utilisations dans le contexte du programme des nouveaux gTLD.

Utilisation malveillante du DNS : terminologie à retenir

L'« utilisation malveillante du DNS » couvre toute une gamme d'activités. Bien qu'il n'existe aucune définition admise à l'échelle mondiale, d'autres définitions incluent le « cybercrime », le « piratage » et, tel que l'ICANN l'a utilisé par le passé, le « comportement malveillant ». Des chercheurs de l'université de Rome et du Global Cyber Security Center classent ces menaces au DNS en trois catégories : la corruption des données, le déni de service et la confidentialité.²

L'« utilisation malveillante du DNS » est le terme utilisé dans le présent rapport qui fait référence à des activités volontairement trompeuses, sournoises ou non sollicitées qui utilisent le DNS et/ou les procédures d'enregistrement de noms de domaine. Il s'agit d'une définition pratique fondée sur l'examen des activités généralement répertoriées dans la littérature comme étant malveillantes ou abusives et qui vise à donner à la CCT-RT un point de départ afin qu'elle précise sa définition de l'utilisation malveillante du DNS dans le cadre de ses travaux. Tel qu'indiqué ci-dessous, certaines activités relèvent de pratiques commerciales de « mauvaise foi » mais pas forcément illégales alors que d'autres constituent des escroqueries pures et simples qui seraient probablement jugées illégales dans la plupart des juridictions à travers le monde. La mesure dans laquelle chaque activité malveillante (décrite ci-dessous) correspond à la définition et peut être analysée du point de vue des neuf sauvegardes visant à atténuer l'utilisation malveillante du DNS dans le cadre du programme des nouveaux gTLD pourra encore être appréciée par la CCT-RT. L'objectif est de fournir une structure de définition pratique permettant de donner un cadre aux futures discussions visant à déterminer si telle ou telle activité devrait être incluse dans ses travaux.

Utilisation malveillante du DNS : tactiques et instruments

Les personnes malveillantes mettent en général à exécution leurs plans via les procédés suivants :³

² Casalicchio, Caselli, and Coletta, “Measuring the Global Domain Name System”, IEEE Network 27, n° 1, (2013) 25-31. doi: 10.1109/MNET.2013.6423188

³ Il convient de noter que les deux premiers procédés indiqués sont généralement les principaux procédés auxquels ont recours les personnes malveillantes. Voir l'étude d'Illumintel, “Potential for Phishing in Sensitive-String Top-Level Domains”, menée pour le Comité du programme des nouveaux gTLD du Conseil d'administration de

- **Domaines en danger** : domaines dans lesquels une personne malveillante s'est immiscée via l'hébergement Web d'un titulaire de nom de domaine.
- **Enregistrements malveillants** : domaines enregistrés par des personnes malveillantes dans le but de procéder à des utilisations malveillantes du DNS.
- **Revendeurs de sous-domaines** : services, dont nombreux sont gratuits et proposent un enregistrement anonyme en dehors d'un service WHOIS, qui permettent aux personnes de procéder à des enregistrements à un troisième niveau en dessous d'un domaine de second niveau détenu par le prestataire de service. Ces revendeurs ne conservent en général pas de données relatives à l'enregistrement ou au correspondant autres que les noms de compte d'utilisateur.⁴
- **Adresses IP** : les attaques par hameçonnage utilisent parfois des adresses IP dans leur URL plutôt que des noms de domaine.
- **URL raccourcis** : technique visant à réduire les adresses de domaine interminables qui peuvent être utilisées par des personnes malveillantes afin de brouiller un nom de domaine et de rediriger ainsi des utilisateurs crédules vers des sites malveillants.⁵

Bien que l'utilisation malveillante puisse prendre un certain nombre de formes, son objectif général consiste à diffuser des **programmes malveillants** afin de perturber des opérations informatiques, de rassembler des informations sensibles ou d'avoir accès à des systèmes informatiques privés.⁶ Les programmes malveillants peuvent mener diverses activités dommageables et prendre un certain nombre de formes. Les programmes les plus diffusés comprennent :

- **Virus** : Programmes malveillants qui mènent un certain nombre d'activités non souhaitées et font que les ordinateurs ne fonctionnent pas correctement, y compris via la création, le déplacement et/ou la suppression de dossiers, et/ou via la consommation de mémoire informatique. Ils se reproduisent souvent

l'ICANN, 21 mai 2015, <https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en>

⁴ Groupe de travail anti-hameçonnage, "Making Waves in the Phisher's Safest Harbor: Exposing the Dark Side of Subdomain Registries," novembre 2008, http://docs.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

⁵ Voir StopTheHacker.com, "The Curse of the URL Shorteners: How Safe Are They?", mis en ligne le 26 février 2016, <https://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/>

⁶ « Groupe consultatif de mise en œuvre de la concurrence, la confiance et le choix du consommateur (IAG-CCT) : recommandations finales sur les mesures à des fins d'examen par la CCT », septembre 2014, <https://newgtlds.icann.org/en/reviews/cct/iag-metrics-final-recs-26sep14-en.pdf>

eux-mêmes et se déplacent à travers des réseaux via des e-mails infectés. On peut citer par exemple les « vers » et les « chevaux de Troie ».⁷

- **Logiciels espions** : Programmes malveillants capables de capturer des informations telles que noms d'utilisateur, mots de passe, informations relatives aux cartes de crédit, habitudes de navigation et e-mails.⁸

Les programmes malveillants sont souvent diffusés à l'aide de **bots**, à savoir des logiciels automatiques codés de façon à fonctionner continuellement afin d'assurer des fonctions malveillantes ou abusives.⁹ Les **réseaux zombies** sont des réseaux de bots utilisant des ordinateurs infectés afin de diffuser des programmes malveillants.¹⁰ Les personnes victimes de ces réseaux zombies ne savent pas que leurs dispositifs sont utilisés à ces fins.

Groupe de travail sur les politiques relatives aux enregistrements frauduleux

En 2010, le groupe de travail sur les politiques en matière d'enregistrements frauduleux de la GNSO (RAPWG) a rédigé un rapport passant en revue les dispositions relatives aux fraudes dans les contrats registre/bureau d'enregistrement. Dans ce rapport, le groupe a développé une définition consensuelle de la fraude. La voici :

La fraude est une action qui : a) cause un préjudice réel et considérable, ou est le prédicat matériel d'un tel préjudice, et b) est illégale ou illégitime, ou est contraire à l'intention et au dessein d'un objectif légitime formulé, si un tel objectif est rendu public.¹¹

Ce groupe est allé plus loin et a établi une distinction entre les fraudes à l'**enregistrement** et les fraudes à l'**utilisation**, les fraudes à l'enregistrement faisant référence à des problèmes survenus lors de l'enregistrement de noms de domaine alors que les fraudes à l'utilisation font elles référence à la façon dont les domaines sont utilisés après l'enregistrement. Leur cadre de définition est tel que suit :

⁷ Kaspersky Lab, "What is a Computer Virus or a Computer Worm?" mis en ligne le 26 février 2016, <http://www.kaspersky.com/internet-security-center/threats/viruses-worms>

⁸ Kaspersky Lab, "What is Spyware?", mis en ligne le 26 février 2016, <http://usa.kaspersky.com/internet-security-center/threats/spyware#.VtCsAJMrJTY>

⁹ Les bots ne sont souvent pas malveillants et assurent des fonctions légitimes. Toutefois, le présent rapport fait uniquement référence à leur forme malveillante. Voir Gabada, Usman, and Sharma, "Techniques to Break the Botnet Attack," International Journal for Research in Emerging Science and Technology 2, n° 1 (mars 2015), <http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug638.pdf>

¹⁰ Ibid.

¹¹ « Rapport final du groupe de travail sur les politiques en matière d'enregistrements frauduleux », mai 2010, <http://gns0.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf>

Les problèmes d'enregistrement sont au cœur des activités liées au nom de domaine menées par les bureaux d'enregistrement et les registres. Celles-ci incluent généralement (mais sans s'y limiter) l'allocation de noms enregistrés, la mise à jour et l'accès aux informations sur l'enregistrement (WHOIS), le transfert, la suppression et la réallocation des noms de domaine, et d'autres activités du même ordre présentées plus en détail ci-dessous. Celles-ci relèvent en général du processus décisionnel de la GNSO. La plupart d'entre elles sont expressément répertoriées dans les contrats de registre comme étant sujettes aux politiques de consensus, et les politiques de consensus existantes doivent s'occuper de ce type de questions.

Le groupe a discuté des activités suivantes en tant qu'éventuelles formes de fraudes à l'enregistrement :

- **Cybersquattage** - l'enregistrement et l'utilisation délibérés et de bonne foi d'un nom qui constitue la marque déposée d'une entité non apparentée, souvent à des fins commerciales (généralement, mais pas exclusivement, via la publicité au coût par clic).
- **Réservation préventive** – lorsqu'une partie obtient certaines informations privilégiées eu égard aux préférences d'un internaute pour l'enregistrement d'un nom de domaine et qu'elle en profite pour enregistrer à titre préventif ce nom de domaine.
- **Sites diffamatoires** – sites Web qui se plaignent des produits ou des services d'une société ou entité et utilisent la marque déposée d'une société dans le nom de domaine (par exemple sociéténulle.exemple). Le groupe craint que ces types de sites puissent porter atteinte aux droits des propriétaires de la marque. Mais le groupe a également noté que dans bien des cas, de tels sites permettent de transmettre en toute légitimité des plaintes et sont protégés dans de nombreuses juridictions par des lois relatives à la liberté d'expression.
- **Noms de domaine trompeurs et/ou offensants** – enregistrement de noms de domaine qui dirigent des consommateurs crédules vers un contenu obscène ou dirigent des mineurs vers un contenu pernicieux ; on parle parfois de « mousetrapping ».
- **Faux avis de renouvellement** – correspondance trompeuse envoyée aux titulaires de nom de domaine par un individu ou une organisation prétendant être ou représenter le bureau d'enregistrement actuel. Ces avis sont envoyés à différentes fins mensongères.
- **Permutation de noms** – utilisation d'outils automatisés afin de permuter la chaîne d'un nom de domaine donné. Alors que les bureaux d'enregistrement utilisent ces outils en toute légitimité afin de suggérer des chaînes alternatives aux bureaux d'enregistrement potentiels lorsque la chaîne que le titulaire de nom de domaine interroge n'est pas disponible, le

groupe craint ici que ces outils engendrent des résultats incompatibles avec les chaînes de marque.

- **Coût par clic** – modèle de publicité Internet utilisé sur des sites Web dans lequel l'annonceur paie l'hôte uniquement lorsque l'on clique sur sa publicité. On craignait ici l'utilisation d'une marque déposée dans un nom de domaine afin de générer du trafic sur un site contenant des publicités à placement payant.
- **Déviation du trafic** – utilisation d'appellations commerciales dans du texte visible avec HTML, du texte caché, des métabalisés ou le titre d'une page Web afin de manipuler les résultats de moteurs de recherche et de dévier le trafic.
- **Fausse affiliation** – prétendre à tort être l'associé du propriétaire d'une marque.
- **Escroquerie d'enregistrement par TLD croisés** – pratique de vente mensongère via laquelle un titulaire de nom de domaine existant reçoit un avis selon lequel une autre partie souhaite ou essaie d'enregistrer la chaîne du domaine d'un titulaire de nom de domaine dans un autre TLD. Le titulaire de nom de domaine est ainsi contraint d'effectuer de nouveaux enregistrements par l'intermédiaire de la partie qui a envoyé l'avis, bien souvent un revendeur qui souhaite tirer profit des nouveaux enregistrements et propose de créer le nouveau domaine à un prix supérieur au prix du marché.
- **Nom de domaine test/planant** – lorsque les titulaires de nom de domaine abusent du « délai de grâce supplémentaire » en procédant en continu à des enregistrements, des suppressions et des réenregistrements des mêmes noms afin d'éviter de payer des frais d'enregistrement..

En revanche, le RAPWG a défini l'« utilisation » de la façon suivante :

L'utilisation des noms de domaine concerne ce qu'un titulaire de nom de domaine fait avec son nom de domaine une fois que le domaine est créé, à savoir la raison pour laquelle le titulaire de nom de domaine crée le domaine et/ou les services qu'il y assure. Cette utilisation n'a souvent rien à voir avec les questions d'enregistrement... [L]'utilisation d'un nom de domaine est une question pour laquelle la compétence de l'ICANN et de la GNSO en matière d'élaboration de politiques est plus limitée. ☒

Le groupe a discuté des activités suivantes en tant qu'éventuelles formes de fraudes à l'utilisation :

- **Hameçonnage** – site Web se présentant à tort comme un site de confiance (souvent une banque) afin de tromper les internautes pour qu'ils fournissent des informations sensibles (par exemple identifiants de connexion bancaire, mots de passe d'e-mails). Généralement,

- l'hameçonnage a pour but de voler des fonds ou d'autres actifs de valeur.
- **Spam** – envoi en masse d'e-mails indésirables depuis des domaines afin de faire la publicité de sites Web.
 - **Commande et contrôle de programmes malveillants/réseaux zombies** – utilisation de noms de domaine de façon à contrôler et mettre à jour les réseaux zombies, qui sont des réseaux de centaines, de milliers ou de millions d'ordinateurs infectés tous sous le contrôle d'un criminel. Les réseaux zombies peuvent être utilisés afin de mener différents types d'activités malveillantes, y compris les **attaques par déni de service distribué (DDOS), le spam et l'hébergement fast-flux** de sites d'hameçonnage et de spam [voir ci-dessous une explication détaillée des pratiques et de la terminologie utilisées dans cette définition].
 - **Utilisation d'identifiants dérobés** – par exemple une identité, des identifiants d'accès et des coordonnées bancaires afin d'enregistrer des noms de domaine à des fins malveillantes, de voler des individus ou organisations et/ou de perturber les opérations d'un individu ou d'une organisation.

Dans le rapport, le RAPWG réitère que l'ICANN et ses différentes organisations de soutien disposent d'une certaine compétence eu égard aux questions d'*enregistrement* via les processus décisionnel et de mise en application, alors qu'il n'est pas facile de répondre aux questions d'*utilisation* au vu de la compétence limitée de l'ICANN concernant la façon dont les titulaires de nom de domaine utilisent leur nom de domaine. Il convient de noter que seules les définitions et activités abordées par les membres du RAPWG aux fins du présent rapport sont présentées dans cette section ; elles ne sauraient constituer une quelconque approbation par l'ICANN des activités qualifiées d'utilisations malveillantes du DNS. Les définitions et activités mentionnées dans le présent rapport sont données afin d'orienter les travaux de la CCT-RT et sont uniquement fournies à titre informatif et afin d'engager des discussions.

Spécification 11 du contrat de registre des nouveaux gTLD

La spécification 11 du contrat de registre des nouveaux gTLD prévoit que les opérateurs de registre s'engagent à respecter certains engagements d'intérêt public (PIC) dans le cadre de leurs obligations contractuelles avec l'ICANN. Les sous-sections 3a et 3b mettent l'accent sur les PIC des opérateurs de registre en tant qu'aspect de l'utilisation malveillante du DNS et décrivent les activités qui devraient être incluses dans leurs initiatives visant à atténuer et assurer un suivi des comportements malveillants dans leurs TLD. La spécification 11 précise ce qui suit :¹²

¹² « Contrats de registre », mis en ligne le 4 février 2016, <https://www.icann.org/resources/pages/registries/registries-agreements-en>

3a. L'opérateur de registre inclura dans son contrat registre/bureau d'enregistrement une disposition en vertu de laquelle les bureaux d'enregistrement doivent inclure dans leurs contrats d'enregistrement une disposition interdisant aux détenteurs de domaines enregistrés 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) les sanctions pour ce type d'activités, y compris la suspension du nom de domaine.

3b. L'opérateur de registre procédera périodiquement à une analyse technique afin d'évaluer si les domaines de son TLD sont utilisés de façon à perpétrer des menaces à la sécurité comme le dévoiement, le hameçonnage, les programmes malveillants et les réseaux zombies. L'opérateur de registre rédigera des rapports statistiques sur le nombre des menaces à la sécurité identifiées et les mesures prises suite aux vérifications périodiques en matière de sécurité. L'opérateur de registre rédigera ces rapports pendant la durée du contrat, sauf si un délai plus court est requis par la loi ou approuvé par l'ICANN, et il les présentera à l'ICANN sur demande.

Les activités décrites à la spécification 11 peuvent fournir un cadre de définition supplémentaire pour la CCT-RT afin de préciser la portée de son examen.

Utilisation malveillante du DNS : autres définitions et considérations

Il convient de noter un certain nombre d'autres termes et considérations eu égard aux activités constituant une utilisation malveillante du DNS :

- L'**hameçonnage** utilise à la fois l'**ingénierie sociale** et des subterfuges techniques pour dérober les coordonnées personnelles et bancaires des internautes. Les mécanismes d'ingénierie sociale utilisent des adresses e-mail usurpées pour diriger les utilisateurs vers des sites Web frauduleux conçus pour piéger les destinataires en les amenant à divulguer des données financières telles que des numéros de carte bancaire, des noms d'utilisateur et mots de passe de leurs comptes et des numéros de sécurité sociale. L'**hameçonnage ciblé** est une forme spécifique d'e-mail frauduleux qui cible des individus occupant des postes importants au sein d'une organisation afin de les amener à fournir des informations sensibles.¹³

¹³ « Avis du SSAC sur la protection des titulaires de noms de domaine : meilleures pratiques pour préserver la sécurité et la stabilité dans le cycle de gestion des informations d'identification », Comité consultatif sur la sécurité et la stabilité de l'ICANN, novembre 2015, <https://www.icann.org/en/system/files/files/sac-074-en.pdf>,

- Le **fast-flux** est une technique utilisée par des réseaux zombies dans le cadre du hameçonnage, du spam et autres activités de diffusion de programmes malveillants via laquelle des attaques sont envoyées à partir d'un ensemble d'adresses IP en constante évolution, la détection étant de ce fait complexe.¹⁴
- Le **typosquattage** est une forme de **cybersquattage** consistant à faire une erreur de frappe lorsque l'on saisit l'adresse d'un site Web sur le navigateur Web et à rediriger les internautes vers des sites malveillants.¹⁵
- Les **publicités malicieuses** (« malvertising ») sont des publicités publiées sur un site Web ou un réseau publicitaire de sorte à infecter les internautes via des programmes malveillants à chaque fois que les publicités sont visualisées ou à différents intervalles en fonction de la fréquence ou du nombre de visites.¹⁶
- L'**empoisonnement des moteurs de recherche** est une activité qui manipule les moteurs de recherche de sorte à afficher des résultats qui renvoient vers des sites Web malveillants.¹⁷
- Les **attaques par usurpation** surviennent lorsqu'une personne malveillante se fait passer pour un autre dispositif ou utilisateur afin de lancer des attaques contre des hôtes du réseau, voler des données, propager des programmes malveillants ou contourner les contrôles d'accès.¹⁸
- Les **attaques par déni de service (distribué) (DDOS)** sont des cyberattaques lancées afin de mettre hors circuit un ou plusieurs systèmes informatiques. On parle d'attaque *distribuée*, c'est-à-dire lancée via un réseau zombie, lorsque de multiples systèmes sont coordonnés de façon à submerger les serveurs des victimes de demandes. Une nouvelle forme d'attaque par DDOS « **amplifiée** » a vu le jour ; elle utilise le reflet et l'amplification du DNS afin d'atteindre des taux binaires de données d'attaques élevées (qui dépasseraient 300 gigabits par seconde) qui excèdent la capacité du réseau d'une victime et entraînent des interruptions totales ou importantes des services.¹⁹

¹⁴ « Avis du SSAC sur l'hébergement fast-flux et le DNS », Comité consultatif sur la sécurité et la stabilité de l'ICANN, mars 2008, <https://www.icann.org/en/system/files/files/sac-025-en.pdf>

¹⁵ Moore and Edelman, “Measuring the Perpetrators and Funders of Typosquatting”, rapport présenté lors de la 14e Conférence internationale sur la cryptographie financière et la sécurité des données, Tenerife, janvier 2010, <http://www.benedelman.org/typosquatting/typosquatting.pdf>,

¹⁶ Quatrième symposium mondial sur la sécurité, la stabilité et la résilience du DNS, compte rendu de réunion, octobre 2012, <https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf>,

¹⁷ “Search Engine Poisoning,” Imperva, mis en ligne le 1er février 2016, https://www.imperva.com/resources/glossary?term=search_engine_poisoning_sep,

¹⁸ Veracode, “Spoofing Attack: IP, DNS & ARP”, mis en ligne le 4 février 2016, <http://www.veracode.com/security/spoofing-attack>

¹⁹ « Avis du SSAC sur les attaques par DDOS affectant l'infrastructure du DNS », Comité consultatif sur la sécurité et la stabilité de l'ICANN, février 2014,

- La **réplication des domaines** est une nouvelle forme d'utilisation malveillante du DNS via laquelle les criminels, à l'aide d'informations d'identification volées ou hameçonnées, créent de nombreux sous-domaines associés aux domaines légitimes existant dans le portefeuille d'un titulaire de nom de domaine. Les domaines légitimes continuent de fonctionner normalement du point de vue du titulaire de nom de domaine tandis que ces sous-domaines dirigent les visiteurs vers des sites malveillants.²⁰
- L'**empoisonnement du cache DNS** est une attaque via laquelle une personne malveillante amène un serveur de nom à ajouter des données malveillantes ou à remplacer les données du DNS en cache par des données malveillantes. Le dévoiement en est une forme ; une personne malveillante amène une victime à cliquer sur un lien, en règle générale envoyé par un pourriel, qui infecte l'ordinateur personnel ou le serveur de la victime et redirige les internautes vers des sites Web frauduleux où des informations personnelles confidentielles peuvent être soutirées.²¹

Un élément clé à ne pas oublier concernant presque toutes ces tactiques est qu'elles profitent des faiblesses de l'être humain telles que la cupidité, la négligence et/ou la naïveté. Ainsi, **les utilisateurs finaux sont en général les maillons faibles de la chaîne de cybersécurité.**²²

Utilisation malveillante du DNS : statistiques clés et principales tendances

Selon une récente étude mondiale parrainée par l'ICANN et menée auprès de 6144 consommateurs :

- 74 % avaient connaissance de l'hameçonnage

<https://www.icann.org/en/system/files/files/sac-065-en.pdf>. Voir également Alvarez, Carlos, "Amplified DDoS Attacks: The Current Biggest Threat Against the Internet", blog de l'ICANN, 11 avril 2014, <https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet>

²⁰ « Avis du SSAC sur la protection des titulaires de noms de domaine : meilleures pratiques pour préserver la sécurité et la stabilité dans le cycle de gestion des informations d'identification », Comité consultatif sur la sécurité et la stabilité de l'ICANN, novembre 2015, <https://www.icann.org/en/system/files/files/sac-074-en.pdf>




²¹ Voir Piscitello, Dave, "DNS Pharming: Someone's poisoned the water hole!", WatchGuard Technologies Expert Editorial, 2005, <http://www.corecom.com/external/livesecurity/dnsphishing.htm>

²² Khonji, Mahmoud and Youssef Iraqi, "Phishing Detection: A Literature Survey," IEEE Communications Surveys & Tutorials 15, n° 4 (Q4 2013), doi: 10.1109/SURV.2013.032213.00009.

- 79 % avaient connaissance de l'envoi de pourriels
- 40 % avaient connaissance du cybersquattage
- 67 % avaient connaissance du vol d'informations d'identification
- 76 % avaient connaissance des programmes malveillants

En plus d'une bonne connaissance des comportements malveillants sévissant au sein du DNS, les utilisateurs finaux ont également déclaré avoir très/assez peur de chacun des comportements malveillants et ont indiqué qu'ils pensaient que ces comportements étaient très/assez courants.²³





Symantec, l'une des plus grandes sociétés spécialisées en cybersécurité au monde, élabore chaque année un rapport sur l'état de la sécurité d'Internet à l'échelle mondiale.²⁴ Son dernier rapport fournit un certain nombre d'indicateurs illustrant les tendances générales des principales activités liées à l'utilisation malveillante du DNS. Il peut servir comme point de départ d'une analyse plus segmentée des utilisations malveillantes du DNS pour les TLD nouveaux et historiques au fur et à mesure de l'avancée des travaux de la CCT-RT :

Indicateur	Statistiques descriptives	Tendance
Sites Web avec programmes malveillants	<ul style="list-style-type: none"> • 2014 : 1 sur 1126 • 2013 : 1 sur 566 	
Taux de spam total (pourcentage de tous les e-mails qualifiés de spams)	<ul style="list-style-type: none"> • 2015 : 54 %²⁵ • 2014 : 60 % • 2013 : 66 % 	
Volume total de spam par jour (estimation)	<ul style="list-style-type: none"> • 2014 : 28 milliards • 2013 : 29 milliards 	

²³ Étude mondiale de l'ICANN menée auprès des consommateurs par Nielsen, avril 2015, <https://www.icann.org/news/announcement-2015-05-29-en>

²⁴ Symantec, « Rapport 20 sur les menaces à la sécurité d'Internet », avril 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

²⁵ Il convient de noter que ce chiffre a été tiré du rapport de situation de Symantec de novembre 2015 disponible sur www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-11-2015-en-us.pdf. Ce chiffre est un chiffre annuel ne prenant pas en compte les données de décembre 2015. Symantec n'a pas communiqué de chiffres pour l'année 2015 pour les autres indicateurs figurant dans ce tableau.

Taux d'hameçonnage d'e-mails (proportion des e-mails qui constituent des tentatives d'hameçonnage)	<ul style="list-style-type: none"> • 2014 : 1 sur 965 • 2013 : 1 sur 392 	
Nouvelles variantes de programme malveillant ajoutées chaque année	<ul style="list-style-type: none"> • 2014 : 317 millions • 2013 : 252 millions 	
Proportion d'e-mails contenant des programmes malveillants	<ul style="list-style-type: none"> • 2014 : 1 sur 244 • 2013 : 1 sur 196 • 2012 : 1 sur 291 	
Nombre de bots :	<ul style="list-style-type: none"> • 2014 : 1,9 million • 2013 : 2,3 millions • 2012 : 3,4 millions 	

Bien que ces données indiquent une tendance générale à la baisse des formes spécifiques d'utilisation malveillante du DNS analysées, il convient de noter qu'elles ne constituent qu'un aperçu de ces tendances. Par exemple, alors que les attaques par hameçonnage semblent diminuer d'après le tableau, le nombre d'attaques par hameçonnage a presque doublé depuis 2008, ce qui laisse penser que la tendance à la baisse pourrait correspondre à une simple diminution dans la courbe de tendance générale.²⁶ De plus, les données présentées concernent l'*ensemble* du DNS ; elles ne décrivent pas uniquement les utilisations malveillantes du DNS pour les nouveaux gTLD.

Utilisation malveillante du DNS pour les nouveaux gTLD

Peu d'études systématiques sur l'utilisation malveillante du DNS pour les nouveaux gTLD ont été menées, ce qui s'explique par leur nouveauté. Selon l'étude parrainée par l'ICANN susmentionnée, **le niveau de confiance des consommateurs dans les nouveaux gTLD est bien plus bas que pour les TLD historiques**, environ 50 % des consommateurs déclarant faire confiance aux nouveaux gTLD alors qu'environ 90 % déclarent faire confiance aux TLD historiques.²⁷ Les chercheurs de l'université de Californie, San Diego, ont révélé qu'**il était deux fois plus probable que les nouveaux TLD figurent sur une liste noire des domaines (liste de domaines de**

²⁶ Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains," étude pour le Comité du programme des nouveaux gTLD du Conseil d'administration de l'ICANN, 21 mai 2015, <https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en>

²⁷ Étude mondiale de l'ICANN menée auprès des consommateurs par Nielsen, avril 2015, <https://www.icann.org/news/announcement-2015-05-29-en>

spammeurs connus) que les TLD historiques, au cours de leur premier mois d'enregistrement.²⁸

Selon les membres de l'APWG, il semble que **les personnes malveillantes testent l'espace des nouveaux gTLD** comme base potentielle pour leurs activités.²⁹ Ils suggèrent que cela pourrait résulter d'un renforcement de la concurrence sur le marché des nouveaux gTLD, dont les prix baissent et qui attire des personnes malveillantes cherchant à tirer profit des bas prix. Toutefois, ils mettent en avant la difficulté de tirer des conclusions sur la base de données comparatives limitées étant donné que les nouveaux gTLD en sont au tout début de leur introduction. Ils recommandent que de nouvelles études soient menées afin de comparer l'utilisation malveillante pour les TLD nouveaux et historiques lorsque suffisamment de données seront disponibles.³⁰

Architelos, société de conseil et gestion des TLD, propose une analyse plus segmentée de l'utilisation malveillante du DNS dans les domaines nouveaux, historiques et géographiques (ccTLD). Son dernier rapport, publié en juin 2015, utilise comme mesure l'indice de qualité de l'espace de noms (NQi), qui correspond à la **proportion de domaines malveillants figurant sur sa liste noire par million de domaines** gérés dans chaque registre, afin d'analyser la situation des comportements malveillants dans les gTLD nouveaux et historiques. Le rapport contient un certain nombre de conclusions importantes :³¹

- Selon le NQi calculé entre janvier 2014 et juin 2015, le taux d'**activités malveillantes** (hameçonnage, programme malveillant, commande et contrôle de réseaux zombies et spam) dans les nouveaux gTLD **a augmenté considérablement** depuis le premier abus détecté dans les nouveaux gTLD en février 2014 et se rapproche du niveau des gTLD historiques.
- **Le spam représente 99 % des abus signalés dans les nouveaux gTLD** pendant la durée de leur analyse (le spam représente 90 % des abus dans les gTLD historiques et les ccTLD).

²⁸ Il convient de noter qu'il s'agit d'une mesure instantanée prise au moment de l'étude qui ne correspond en aucun cas à une analyse à long terme. Voir Der et al., "From .academy to .zone: An Analysis of the New TLD Land Rush," département des sciences informatiques et de l'ingénierie de l'université de Californie, San Diego, octobre 2015, doi: 10.1145/2815675.2815696.

²⁹ Groupe de travail anti-hameçonnage, "Global Phishing Survey: Trends and Domain Name use in 1H2014", 25 septembre 2014, <https://apwg.org/apwg-news-center/>

³⁰ Ibid.

³¹ Architelos, "The NameSentry Abuse Report", juin 2015, <http://architelos.com/wp-content/uploads/2015/06/Architelos-StateOfAbuseReport2015-webc-FIN.pdf>

- En mai 2015, **le NQI s'élevait, pour les nouveaux gTLD, à 11 654 par million de domaines** gérés contre environ **16 500 par million pour les gTLD historiques**.
- **Les taux d'hameçonnage, de programmes malveillants et de commande et contrôle de réseaux zombies dans les nouveaux gTLD sont toujours très bas** par rapport aux gTLD historiques, bien qu'il soit très probable qu'ils augmentent de pair avec une hausse de l'adoption des nouveaux gTLD et de la sensibilisation à l'égard de ces derniers. De mai 2014 à mai 2015, **le nombre de domaines hameçonnés est passé de 7 à 143**, ce chiffre ayant donc été multiplié par 20 (ce chiffre étant lui passé de 7300 à 14 000 pour les gTLD historiques sur la même période). Toutefois, **77 % de ces 143 nouveaux cas d'hameçonnage ne concernent que dix nouveaux gTLD**.

Étude de cas sur l'utilisation malveillante du DNS : l'hameçonnage des nouveaux gTLD

La prévalence de l'hameçonnage est un indicateur de la mesure dans laquelle les personnes malveillantes abusent des nouveaux gTLD. Une étude menée par des membres de l'APWG souligne qu'**il est peu probable que le développement du DNS via le programme des nouveaux gTLD fasse augmenter le nombre d'hameçonnages dans le monde**, mais il créera de **nouveaux emplacements à partir desquels les attaques par hameçonnage pourront survenir**, dans la mesure où les cybercriminels ont parfois tendance à passer d'un TLD à l'autre.³² En règle générale, les hameçonneurs n'enregistrent pas de domaines qui ont des noms de marque et préfèrent des chaînes illogiques ou placent un nom de marque quelque part dans un sous-domaine ou sous-répertoire, étant donné que les propriétaires de marque cherchent régulièrement à savoir si leurs noms n'ont pas été utilisés de façon inappropriée. Pour la seconde moitié de 2014, seul 1,9 % de l'ensemble des domaines utilisés pour l'hameçonnage contenait un nom de marque ou une variante (ils étaient souvent mal orthographiés).

Dans le cadre d'une autre analyse menée par les membres de l'APWG, ces derniers sont arrivés à une conclusion analogue, à savoir que les nouveaux gTLD ne constituent pas un nouveau filon pour les hameçonneurs. Les auteurs des deux rapports utilisent une mesure, « le nombre de domaines hameçonnés sur 10 000 domaines », qui correspond au rapport entre le nombre de noms de domaines utilisés pour l'hameçonnage dans un TLD et le nombre de noms de domaine enregistrés dans

³² Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains," étude pour le Comité du programme des nouveaux gTLD du Conseil d'administration de l'ICANN, 21 mai 2015, <https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en>

ce TLD, afin d'évaluer la santé des nouveaux TLD en matière d'hameçonnage.³³ Dans leur analyse, ils sont arrivés à la conclusion qu'un score **entre 3,4 et 4,7 domaines hameçonnés sur 10 000 domaines représente un niveau de prévalence du hameçonnage moyen**.³⁴ Un score supérieur à 4,7 indiquerait qu'un TLD aurait des niveaux d'hameçonnage supérieurs à la moyenne. Pour la seconde moitié de 2014, le nombre moyen de domaines hameçonnés sur 10 000 domaines s'élevait à 3,4 pour l'ensemble des TLD. **Seuls neuf des 295 nouveaux gTLD (en 2014) présentaient un score supérieur à 3,4**.³⁵ De plus, **la durée de vie moyenne des attaques par hameçonnage** (ou le temps d'activité de ces attaques et une mesure clé de la puissance des initiatives des hameçonneurs) **se situe à un niveau historiquement bas**, ce qui prouve que **les mesures anti-hameçonnage ont eu un relatif succès**.³⁶

Selon les auteurs des deux rapports, **le prix des domaines semble jouer un rôle important dans l'hameçonnage** des TLD, et les domaines ont tendance à être moins chers dans les TLD historiques.³⁷ Ce sentiment a été confirmé par un certain nombre de représentants des registres et bureaux d'enregistrement lors d'une téléconférence parrainée par l'ICANN sur la mesure de l'utilisation malveillante du DNS, qui a indiqué que **le prix élevé des domaines constituait un facteur clé de réduction des activités malveillantes en général**.³⁸ Selon les membres de l'APWG, plus la prévalence des nouveaux gTLD sera marquée et plus les prix chuteront en raison d'une augmentation de l'offre et d'un renforcement de la concurrence, plus fort sera le risque d'hameçonnage pour ces nouveaux gTLD par rapport aux TLD historiques et géographiques (ccTLD). Un élément d'information attestant de cette tendance est le cas du gTLD .xyz, qui a offert des domaines gratuits pendant un certain temps. Pendant la seconde moitié de 2014, près de 2/3 de l'hameçonnage des nouveaux gTLD

³³ Groupe de travail anti-hameçonnage, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 mai 2015, <https://apwg.org/apwg-news-center/>

³⁴ Il convient de noter que le rapport de l'APWG pour la première moitié de 2014 indiquait un score entre 4,1 et 4,7. Ces mesures changent en fonction de la « courbe » de l'ensemble des activités d'hameçonnage.

³⁵ Groupe de travail anti-hameçonnage, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 mai 2015, <https://apwg.org/apwg-news-center/>

³⁶ La durée de vie *moyenne* a légèrement augmenté lors de la seconde moitié de 2014, passant de 8 heures et 42 minutes à 10 heures et 6 minutes. Voir le groupe de travail anti-hameçonnage, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 mai 2015, <https://apwg.org/apwg-news-center/>

³⁷ Groupe de travail anti-hameçonnage, "Global Phishing Survey: Trends and Domain Name use in 2H2014," 27 mai 2015, <https://apwg.org/apwg-news-center/>

³⁸ C'est lorsqu'un participant fixe un seuil supérieur à 15 US\$ pour un domaine que les taux d'abus commencent à décliner. Opérations et politiques de recherche de l'ICANN, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 janvier 2016, délibérations de la téléconférence, enregistrements disponibles sur <https://newgtlds.icann.org/en/reviews/dns-abuse>

étaient concentrés sur le registre .xyz.³⁹ La réduction des coûts semble être un enjeu important pour les hameçonneurs, les études révélant que l'hameçonnage est une « activité peu qualifiée et peu valorisante »⁴⁰ Bien qu'il y ait eu des cas de gains spectaculaires suite à une attaque par hameçonnage, l'hameçonneur moyen peut gagner en général quelques centaines de dollars par semaines.⁴¹

Les neuf sauvegardes

Avant le lancement du programme des nouveaux gTLD, l'ICANN a demandé l'avis d'experts en matière d'utilisation malveillante du DNS et de cybersécurité afin de recommander des mesures préventives susceptibles de réduire l'exercice des activités susmentionnées. La communauté d'experts a dégagé les neuf sauvegardes présentées ci-dessous. Il reste maintenant à la CCT-RT de déterminer la mesure dans laquelle ces sauvegardes ont permis d'atteindre les objectifs affichés.

Afin de comprendre l'« efficacité » des neuf sauvegardes en termes de réduction de l'utilisation malveillante du DNS, **le terme efficacité doit dans un premier temps être défini en tant que concept mesurable.** Les pages suivantes aborderont ces définitions dans le contexte de chacune des questions posées dans le cadre des premières initiatives visant à déterminer les types de sauvegardes qui seraient nécessaires pour le programme des nouveaux gTLD. Les données disponibles relatives aux mesures de l'« efficacité » proposées seront présentées. Si aucune donnée n'est disponible, s'engagera une discussion sur les raisons de cette absence de données et sur les autres éventuels moyens d'évaluer l'efficacité d'une sauvegarde donnée.

Question : Comment s'assurer que des personnes malveillantes n'exploitent pas de registres ?

L'« efficacité », dans le cadre de cette question, peut être entendue comme la capacité d'empêcher les personnes malveillantes, telles que celles condamnées à un délit ou un crime lié à des activités financières, d'exploiter des registres. Dès 2001, le contrat

³⁹ Les auteurs soulignent que la plupart des enregistrements par hameçonnage .xyz ont été effectués via des bureaux d'enregistrement chinois et utilisés afin d'attaquer des cibles chinoises. Voir le groupe de travail anti-hameçonnage, “Global Phishing Survey: Trends and Domain Name use in 2H2014,” 27 mai 2015, <https://apwg.org/apwg-news-center/>

⁴⁰ Herley and Florencio, “A Profitless Endeavor: Phishing as Tragedy of the Commons,” Microsoft Research, septembre 2008, <http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf>

⁴¹ Ibid. Au vu de sa nature clandestine, il est difficile d'obtenir des données. De ce fait, un vif débat se tient sur les coûts et bénéfices réels de l'hameçonnage en général.

de registre .COM stipulait que la résiliation du contrat de registre serait possible si un opérateur de registre :

« (a) était déclaré coupable par un tribunal de la juridiction compétente d'un crime ou d'un autre délit grave lié à des activités financières, ou avait fait l'objet d'une décision de justice que l'ICANN estime équivaloir en substance à l'une de ces fautes ; ou (b) était puni par le gouvernement de son lieu de résidence pour conduite impliquant un acte malhonnête ou un détournement des fonds d'autrui. »⁴²

Cette clause existe également dans le contrat de registre des nouveaux gTLD, ainsi que d'autres dispositions :

(f) L'ICANN peut, suite à un préavis adressé à l'opérateur de registre, résilier ce contrat si (i) l'opérateur de registre emploie délibérément un cadre qui a été reconnu coupable d'un crime ou d'un délit lié à des activités financières ou de tout autre crime, ou s'il a été jugé coupable de fraude ou de manquement à un devoir fiduciaire par un tribunal de juridiction compétente, ou s'il a fait l'objet d'une décision judiciaire que l'ICANN estime équivaloir en substance à l'un des cas ci-dessus et que ce cadre n'est pas congédié dans les trente (30) jours civils à compter du moment où les faits ci-dessus ont été portés à la connaissance de l'opérateur de registre, ou (ii) si un membre du conseil d'administration ou de l'organe de direction équivalent de l'opérateur de registre a été reconnu coupable d'un crime ou d'un délit lié à des activités financières ou de tout autre crime, ou a été jugé par un tribunal de juridiction compétente coupable de fraude ou de manquement à un devoir fiduciaire, ou a fait l'objet d'une décision judiciaire que l'ICANN estime équivaloir en substance à l'un des cas ci-dessus et que ce membre n'est pas démis de ses fonctions de membre du Conseil d'administration ou de l'organe de direction équivalent de l'opérateur de registre dans les trente (30) jours civils à compter du moment où les faits ci-dessus ont été portés à la connaissance de l'opérateur de registre.⁴³

Sauvegarde : vérification des opérateurs de registre

Contexte

La vérification des opérateurs de registre avant l'exécution d'un contrat de registre et la délégation d'un TLD dans la zone racine a été ajoutée en tant que sauvegarde au guide de candidature aux gTLD pour le programme des nouveaux gTLD afin

⁴² « Contrat de registre .com », 25 mai 2001, <https://www.icann.org/resources/unthemed-pages/registry-agmt-com-2001-05-25-en#II-16C>.

⁴³ « Contrats de registre », 9 janvier 2014, <https://www.icann.org/resources/pages/registries/registries-agreements-en>

d'empêcher les candidats ayant des antécédents en matière de comportements criminels ou malicieux d'exploiter des TLD. Cette mesure a été définie dans le but de créer un processus visant à vérifier les opérateurs de registre avant de conclure un contrat de registre lors de l'évaluation initiale des candidatures.

L'ICANN a engagé PricewaterhouseCoopers (PwC) afin de réaliser les vérifications d'antécédents dans deux domaines précis : (1) le contrôle de l'activité professionnelle et des antécédents criminels ; (2) les antécédents de cybersquattage. L'éligibilité d'un candidat à prendre part au programme des nouveaux gTLD a été communiquée lors de l'évaluation initiale et parfois dans des rapports d'évaluation approfondie.

La vérification des antécédents utilisée dans le programme des nouveaux gTLD est effectuée à un moment donné lors du processus d'évaluation initiale. Si un candidat fait part de modifications à ses informations relatives à la candidature lors de l'évaluation, une nouvelle vérification des antécédents sera effectuée avant la conclusion du contrat de registre. Dans tous les cas, l'ICANN s'est réservée le droit d'effectuer un autre contrôle préalable, si besoin est, avant la conclusion d'un contrat.

Définition de l'« efficacité »

Pour cette sauvegarde, l'efficacité peut être définie comme la capacité d'empêcher les personnes malveillantes ayant des antécédents en matière de comportements malicieux ou criminels de conclure un contrat de registre avec l'ICANN. Toutefois, comme vu précédemment, un processus de contrôle s'effectue à un moment donné, et des changements peuvent survenir au sein de l'entité chargée de la gestion d'un TLD (par exemple une société peut être vendue ou un cadre peut être remplacé). Eu égard à l'utilisation malveillante du DNS, il peut aussi être important de déterminer régulièrement s'il existe des preuves de personnes malveillantes exploitant des registres ou un risque d'une telle exploitation.

Contexte actuel

Conformément à l'évaluation de la mise en œuvre du programme publiée en janvier 2016, le processus de vérification des antécédents constituait une « évaluation menée auprès de toutes les entités candidates et de tous les individus et organisations divulgués aux questions 9-11 de la candidature, cadres et directeurs des entités candidates compris, en plus des actionnaires détenant une importante participation dans l'entité ». ⁴⁴ Selon l'évaluation, l'ICANN a effectué 1150 vérifications d'antécédents sur 1930 candidatures (certaines entités ont soumis plusieurs candidatures). Les résultats des vérifications d'antécédents pour chaque candidature ont été communiqués une fois les procédures d'évaluation initiale achevées. Dans certains cas, des questions supplémentaires ont été posées aux candidats par le panel de vérification des antécédents. Globalement, il est ressorti de l'évaluation de la mise

⁴⁴ « Évaluation de la mise en œuvre du programme », 29 janvier 2016, <https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf>

en œuvre du programme que la vérification des antécédents avait été un succès dans la mesure où tous les candidats ont pu être passés au crible ; toutefois, le délai entre la soumission de la candidature et la conclusion des contrats de registre était plus long que prévu. De ce fait, bon nombre de candidats ont dû être de nouveau passés au crible. L'évaluation laisse penser que les vérifications d'antécédents pourraient être menées au moment de la conclusion du contrat plutôt que lors de l'évaluation initiale afin de réduire la nécessité de procéder à une deuxième vérification.

Possibles méthodes de collecte et mesure des données

Il est peut-être trop tôt pour déterminer si *les deux* aspects de la sauvegarde ont été efficaces en tant que mesures préventives. Toute mesure de l'« efficacité » devrait prendre en compte les données relatives aux rejets des candidatures sur la base de la vérification initiale des antécédents ainsi qu'aux résiliations des contrats de registre du fait de l'incapacité du registre à supprimer les personnes malveillantes de son personnel ou conseil d'administration. Et en raison des informations personnelles dévoilées et du caractère sensible du processus de vérification des antécédents, les rapports indiquant si les candidatures ont été admissibles à l'étape suivante du processus sont limités. Toutefois, les chiffres globaux sont disponibles. Les plaintes formelles en matière de conformité et/ou les résiliations des contrats de registre pourraient donner une indication de l'efficacité de cette sauvegarde sur le long terme.

En outre, la sauvegarde peut avoir eu un effet dissuasif sur les éventuels candidats aux antécédents douteux. Toutefois, il est presque impossible d'en mesurer l'effet dissuasif, c'est-à-dire le nombre d'individus n'ayant finalement pas soumis de candidatures, dans la mesure où un tel effet ne génère pas de données mesurables.

Question : Comment garantir l'intégrité et l'utilité des informations de registre ?

À cet égard, l'efficacité peut être entendue comme l'utilisation fructueuse de sauvegardes afin d'aider à valider et protéger les informations de registre. Les trois sauvegardes préventives suivantes ont été conçues à cette fin.

Sauvegarde : fourniture d'un plan établi pour le déploiement des DNSSEC

Contexte

Les extensions de sécurité du système des noms de domaine (DNSSEC) ont été développées afin de limiter les tentatives de piratage du processus de consultation du DNS par des personnes malveillantes. Ces personnes malveillantes peuvent s'introduire dans les recherches du navigateur Web d'un internaute et, par exemple, le diriger vers des sites Web malveillants afin de subtiliser des informations confidentielles. Les DNSSEC protègent contre de telles attaques en apposant une signature numérique aux données de sorte à garantir aux utilisateurs la validité de la

source de ces données. Elles utilisent des signatures cryptographiques pour les enregistrements DNS existants afin de vérifier qu'un enregistrement DNS provient bien de son serveur de nom officiel et qu'il n'a pas été altéré à un moment donné.⁴⁵ Le déploiement des registres des DNSSEC permet aux titulaires de nom de domaine d'attribuer des clés de nom de domaine spécifiques à leurs domaines s'ils le souhaitent. Imposer les DNSSEC via le contrat de registre avait pour but d'assurer son déploiement rapide et à grande échelle.

La sauvegarde impose à tous les candidats aux nouveaux gTLD de disposer d'un plan précis pour le déploiement des DNSSEC. Cette exigence est évaluée lors du processus d'évaluation initiale, le but premier étant de réduire le risque d'usurpation des enregistrements DNS. En vertu du contrat de registre, les opérateurs de registre des nouveaux gTLD sont tenus de signer les fichiers de zone des TLD avec les DNSSEC, de suivre les meilleures pratiques décrites dans le RFC 4641 du groupe de travail de génie Internet (IETF) et ses successeurs, d'accepter les éléments à clé publique des noms de domaine enfants de manière sécurisée et de publier les déclarations de pratiques des DNSSEC (DPS) sous le format indiqué dans le RFC 6841.^{46 47}

Définition de l'« efficacité »

L'« efficacité » de cette sauvegarde peut être définie de nombreuses façons. Elle peut simplement être définie comme le fait qu'un opérateur de registre dispose d'un plan précis pour le déploiement des DNSSEC et ait passé l'évaluation au moment de la candidature. Elle peut également être définie en fonction du nombre de problèmes soulevés eu égard au respect par les registres des exigences relatives aux DNSSEC. Enfin, elle peut être définie comme la diffusion plus large des DNSSEC, en se basant par exemple sur le nombre de signatures apposées par les titulaires de nom de domaine ou sur le développement des résolveurs DNS validant les DNSSEC au sein des réseaux exploités par des fournisseurs de services Internet (FSI).⁴⁸

⁴⁵ « DNSSEC – What Is It and Why Is It Important? », mis en ligne le 1er février 2016, <https://www.icann.org/resources/pages/dnssec-qa-2014-01-29-en> ; « How DNSSEC Works », mis en ligne le 1er février 2016, <https://www.cloudflare.com/dnssec/how-dnssec-works/>

⁴⁶ Contrat de registre de l'ICANN, spécification 6 : 1.2 DNSSEC, mis en ligne le 1er février 2016, <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>

⁴⁷ Le « RFC » est une série de documents « Appel à commentaires » élaborés par l'IETF qui contiennent des informations techniques et organisationnelles relatives aux réseaux, aux protocoles, aux procédures et aux concepts informatiques. Voir www.ietf.org/rfc.

⁴⁸ « Guide de déploiement : les DNSSEC pour les fournisseurs de services Internet (FSI) », mis en ligne le 1er février 2016, <http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/>

Contexte actuel

Au 23 février 2016, 1073 TLD sur 1236 TLD (ccTLD compris) dans la zone racine avaient signé les clés DNSSEC.⁴⁹

Possibles méthodes de collecte et mesure des données

À l'heure actuelle, les deux mesures suivantes sont disponibles : le nombre des TLD dans la zone racine et le nombre de domaines de second niveau ayant des clés signées.⁵⁰ Des mesures plus approfondies pourraient se concentrer sur la mesure des problèmes de DNSSEC découverts lors des tests de pré-délégation, sur le nombre de problèmes de suivi des conventions de service (SLA) signalés et le nombre de plaintes reçues en matière de conformité des DNSSEC.

Une mesure complète de l'efficacité dans ce domaine devrait prendre en compte le fait que les bureaux d'enregistrement, les titulaires de nom de domaine, les fournisseurs d'hébergement DNS et les FSI jouent tous un rôle majeur dans le déploiement complet des DNSSEC et leur fonctionnement. À titre d'exemple, bien que les opérateurs de registre soient tenus de disposer d'un plan pour le déploiement des DNSSEC, cela ne signifie pas forcément que les titulaires de nom de domaine l'approuveront. Les données préliminaires recueillies par les services techniques de l'ICANN indiquent que bien souvent seul un faible pourcentage des domaines de second niveau a signé les clés DNSSEC (bien que cela varie considérablement selon les TLD).⁵¹ Une étude de cas qu'il conviendrait de mener concerne CloudFare, une société offrant des services de serveur de nom de domaine et du contenu DNS, qui a décidé de permettre à toute personne de son réseau de sécuriser le trafic avec des DNSSEC en une seule et unique étape. Une étude de cas qui adopterait une approche pluridisciplinaire eu égard au soutien apporté aux DNSSEC par les registres, les bureaux d'enregistrement, le DNS, les fournisseurs d'hébergement et les FSI permettrait d'identifier les lacunes du déploiement des DNSSEC entre les gTLD. Le groupe de travail chargé du déploiement des DNSSEC s'occupe déjà du recueil de ses informations et rédige des rapports disponibles sur dnssec-deployment.org.

Sauvegarde : interdiction des caractères génériques

Contexte

Cette recommandation impose des contrôles adéquats afin d'interdire les caractères génériques du DNS. Cette question se pose dans le cas où, au lieu de donner une

⁴⁹ « Rapport sur les DNSSEC de TLD », mis en ligne le 23 février 2016, http://stats.research.icann.org/dns/tld_report/

⁵⁰ Voir « Rapport sur le déploiement des DNSSEC », mis en ligne le 23 février 2016, <http://rick.eng.br/dnssecstat/>

⁵¹ Données recueillies par les services techniques de l'ICANN à partir de fichiers de zone mis à la disposition du public aux fins du présent rapport.

réponse « erreur de nom » pour des requêtes DNS inexistantes, les opérateurs de registre utilisent la redirection du DNS, les caractères génériques ou les réponses synthétisées.⁵² L'ICANN a interdit ces actions suite à certaines conclusions laissant penser qu'elles feraient courir un risque à la sécurité et la stabilité du DNS en créant de nouvelles opportunités d'attaques malveillantes.⁵³

Cette sauvegarde est définie à la section 2.2 de la spécification 6 du contrat de registre :

2.2. Prohibition des caractères génériques. Pour les noms de domaine qui ne sont pas enregistrés ou pour lesquels le titulaire de nom de domaine n'a pas fourni d'enregistrements valides tels que des enregistrements NS à lister dans le fichier de zone DNS, ou dont le statut ne leur permet pas d'être publiés dans le DNS, l'utilisation d'enregistrements de ressources avec caractères génériques DNS, tel que décrit dans les RFC 1034 et 4592, ou toute autre méthode ou technologie permettant de synthétiser des enregistrements de ressources DNS ou d'utiliser la redirection dans le DNS par le registre, est interdite. Lorsque de tels noms de domaine reçoivent des requêtes, les serveurs de noms publics faisant autorité doivent renvoyer une réponse « erreur de nom » (également appelée NXDOMAIN), RCODE 3, telle que décrite dans le RFC 1035 et dans les RFC associés. Cette disposition s'applique à tous les fichiers de zone du DNS, à tous les niveaux de l'arborescence DNS pour lesquels l'opérateur de registre (ou un affilié engagé dans la prestation de services d'enregistrement) met à jour des données, organise une telle mise à jour ou perçoit des revenus sur cette mise à jour.

Toutefois, en 2014, dans le contexte du cadre de gestion de l'occurrence de collisions de noms de domaine, des caractères génériques ont été déployés dans certains TLD pour une période limitée immédiatement après la délégation du TLD (la période d'interruption contrôlée) afin d'identifier toute collision dans l'espace de noms.⁵⁴ Tel

⁵² «About Wildcard Prohibition (Domain Redirect)», mis en ligne le 1er février 2016, <https://www.icann.org/resources/pages/wildcard-prohibition-2014-01-29-en>

⁵³ Comité consultatif sur la sécurité et la stabilité de l'ICANN, « SAC041 : Recommandation visant à interdire l'utilisation de la redirection et des réponses synthétisées par les nouveaux TLD », 10 juin 2009, <https://www.icann.org/en/system/files/files/sac-041-en.pdf>

⁵⁴ Voir « Foire aux questions : Cadre de gestion de l'occurrence de collisions de noms de domaine pour les registres », mise en ligne le 11 février 2016, www.icann.org/resources/pages/name-collision-ro-faqs-2014-08-01-en, selon lequel : « L'interdiction des caractères génériques est levée lors de la période d'interruption contrôlée pour les TLD concernés (c'est-à-dire s'il n'y a pas de noms actifs en vertu du TLD autres que « nic »). Cette levée s'applique uniquement si aucun nom n'est délégué (et n'est donc actif) dans ce TLD, supprimant les risques traditionnellement associés à

qu'indiqué dans le rapport de la phase 1 de JAS sur la *réduction du risque de collisions dans l'espace de noms du DNS* :

Nous recommandons que le registre mette en œuvre la période d'interruption contrôlée immédiatement après la délégation dans la zone racine et que l'interdiction des enregistrements de caractères génériques soit suspendue lors de cette période. Vu l'objectif d'interruption contrôlée et le fait qu'aucune donnée de titulaire de nom de domaine ne se trouvera dans la zone à ce moment-là, nous estimons qu'autoriser provisoirement les enregistrements de caractères génériques à cette fin ne va pas à l'encontre des interdictions posées par l'ICANN concernant les enregistrements de caractères génériques et ne renforce pas les craintes qui ont mené l'ICANN à poser ces interdictions.⁵⁵

Définition de l'« efficacité »

Pour cette mesure, l'« efficacité » pourrait en théorie être définie en faisant référence au degré de conformité avec l'interdiction des caractères génériques dans les nouveaux gTLD. L'examen de ce comportement en tant que moyen de garantir l'intégrité et l'utilité des informations de registre peut également être envisagé. Les données relatives à l'impact sur les comportements que cette sauvegarde avait pour but de prévenir pourraient également être examinées.

Contexte actuel

L'ICANN met à disposition un formulaire de plainte relative à l'interdiction des caractères génériques (redirection d'un domaine) afin de permettre de signaler des cas de non-conformité aux dispositions contractuelles.⁵⁶ Jusqu'à présent, l'ICANN n'a reçu aucune plainte relative à l'interdiction des caractères génériques via cet outil.⁵⁷

la mise en œuvre de caractères génériques. Cette levée de l'interdiction et la possibilité d'utiliser un caractère générique s'expliquent par la volonté de détecter toutes les situations de collision de noms évidentes. Le caractère générique en « haut » de la zone correspondra à l'ensemble des requêtes qui seront détectées une fois que la zone fonctionnera à plein régime. Cette approche maximise les étapes visant à protéger les internautes actuellement victimes de fuites de requêtes censées être locales. »

⁵⁵ JAS Global Advisors, “Mitigating the Risk of DNS Namespace Collisions”, 4 juin 2014, <https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf>

⁵⁶ Voir « Formulaire de plainte relative à l'interdiction des caractères génériques (redirection d'un domaine) », mis en ligne le 11 février 2016, <https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form>

⁵⁷ Toutefois, le département de la conformité contractuelle a reçu quelques plaintes concernant « les noms réservés/l'interruption contrôlée ». Voir “ICANN Contractual

Possibles méthodes de collecte et mesure des données

Tel que vu précédemment, aucune plainte n'a été reçue des registres de nouveaux gTLD concernant les caractères génériques. Une enquête qualitative auprès des experts techniques sur l'efficacité de cette sauvegarde pourrait être un bon moyen de contourner cette absence de données quantitatives.

Une autre approche pourrait consister à examiner non seulement les plaintes reçues par l'ICANN concernant l'interdiction des caractères génériques dans les TLD concernés mais également la prévalence actuelle de l'utilisation de la redirection du DNS à des fins de « monétisation du trafic d'erreurs », pratique consistant à rediriger les utilisateurs du DNS vers des serveurs Web spécialisés dans la publicité lorsque leurs recherches sur le DNS échouent. Le Netalyzr de l'ICSI de Berkeley, université de Californie, est un outil de diagnostic de réseau ainsi qu'une partie d'une étude de mesure visant à faire le point sur la santé de l'Internet. Il a été utilisé dans de précédentes études passant en revue les problèmes de redirection du DNS et peut être un précieux outil permettant de comprendre les implications des caractères génériques dans le DNS.⁵⁸

Sauvegarde : suppression des enregistrements orphelins de type glue

Contexte

Cette sauvegarde a été développée afin de réduire le risque que des personnes malveillantes introduisent des liens vers des domaines malveillants dans la zone racine via des enregistrements « orphelins de type glue », qui sont des enregistrements de serveur de nom qui peuvent subsister après qu'un enregistrement « parent » a été retiré de la zone. Les enregistrements orphelins de type glue peuvent permettre à des personnes malveillantes de prendre le contrôle de serveurs de nom, ce qui leur donne ensuite la possibilité de mener des activités malveillantes à partir de domaines en apparence « légitimes ». Par exemple, les attaques par « fast-flux » sont connues pour avoir recours à des enregistrements orphelins de type glue afin d'héberger des domaines malveillants pour de courtes périodes.⁵⁹

Compliance Dashboard for 2016”, mis en ligne le 12 février 2016,

<https://features.icann.org/compliance/dashboard/0116/report>

⁵⁸ Weaver, Kreibich, and Paxson, “Redirecting DNS for Ads and Profit”, Atelier d'USENIX sur les communications libres et ouvertes sur l'Internet (FOCI), 2011,

<http://www.icir.org/christian/publications/2011-foci-dns.pdf>

⁵⁹ Voir l'« Avis sur l'hébergement fast-flux et le DNS » du Comité consultatif sur la sécurité et la stabilité de l'ICANN, mars 2008,

<https://www.icann.org/en/system/files/files/sac-025-en.pdf>

La sauvegarde impose aux opérateurs de registre de fournir un plan dans leur dossier de candidature visant à supprimer les enregistrements orphelins de type glue après la suppression de l'enregistrement parent. Après avoir accepté les conditions du contrat de registre, les opérateurs de registre sont tenus de prendre des mesures afin de supprimer les enregistrements orphelins de type glue conformément à la spécification 6, section 4.2 du contrat qui prévoit ce qui suit : « L'opérateur de registre prendra des mesures afin de supprimer les enregistrements orphelins de type glue... lorsqu'il détiendra la preuve par écrit que ces enregistrements sont présents dans le cadre d'une conduite malveillante ». ⁶⁰

Définition de l'« efficacité »

Pour cette mesure, l'« efficacité » peut être entendue comme correspondant aux pratiques réglementées des registres visant à fournir des points de contact pour les utilisateurs finaux afin de signaler des abus et confirmer la suppression automatique des enregistrements orphelins de type glue lorsqu'un enregistrement parent est supprimé de la zone.

Contexte actuel

Selon les premiers feedbacks de la communauté à cet égard, les enregistrements orphelins de type glue en tant que sources d'abus ont été largement neutralisés via des pratiques habituelles consistant à les supprimer des fichiers de zone ; ils restent toutefois un problème mineur dans certains cas. ⁶¹

Possibles méthodes de collecte et mesure des données

L'ICANN a reçu des premiers feedbacks suggérant que cette sauvegarde soit mesurée en utilisant des fichiers de zone afin d'assurer le suivi de la suppression des enregistrements orphelins de type glue au fil du temps.

Le fait d'engager des discussions avec les opérateurs de registre concernant la prévalence et l'utilisation des enregistrements orphelins de type glue à des fins malveillantes pourrait fournir une mesure qualitative permettant de savoir si les registres, les bureaux d'enregistrement et les titulaires de nom de domaine utilisent efficacement les mécanismes requis pour la suppression des enregistrements orphelins de type glue. La « preuve par écrit » requise pour qu'un opérateur de registre supprime les enregistrements orphelins de type glue tel que prescrit par la

⁶⁰ Voir le « Commentaire relatif aux enregistrements orphelins de type glue dans la version préliminaire du guide de candidature » du Comité consultatif sur la sécurité et la stabilité de l'ICANN, mai 2011, <https://www.icann.org/en/system/files/files/sac-048-en.pdf>.

⁶¹ Opérations et politiques de recherche de l'ICANN, “Reviewing New gTLD Program Safeguards Against DNS Abuse,” 28 janvier 2016, délibérations de la téléconférence, enregistrements disponibles sur <https://newgtlds.icann.org/en/reviews/dns-abuse>

spécification 6 peut également fournir une source de données utile. Elle peut aussi être utile afin de localiser des exemples de recommandations visant à supprimer les enregistrements orphelins de type glue dans des politiques de lutte contre les enregistrements frauduleux. À titre d'exemple, le TLD « .rich » comprend une section portant sur la suppression des enregistrements orphelins de type glue dans ses politiques de lutte contre les enregistrements frauduleux,⁶² tandis qu'Afilias traite cette question en tant qu'élément de l'hébergement fast-flux.⁶³

Question : Comment veiller à ce que les initiatives mises en place se concentrent davantage sur la lutte contre les utilisations malveillantes identifiées ?

Cette question porte sur la disponibilité des informations afin de limiter les activités des personnes malveillantes identifiées et afin de les localiser dans le DNS.

Sauvegarde : exigence concernant les enregistrements WHOIS détaillé

Contexte

Cette sauvegarde impose aux nouveaux gTLD de fournir et de maintenir un accès aux enregistrements « WHOIS détaillé » afin d'aider à renforcer la disponibilité et l'exhaustivité des données WHOIS. Les enregistrements WHOIS détaillé sont des enregistrements détenus par les registres « contenant les coordonnées du titulaire du nom de domaine, de son contact administratif et de son contact technique, qui viennent s'ajouter aux informations concernant le bureau d'enregistrement et l'état de l'enregistrement. »⁶⁴ On les oppose aux enregistrements « WHOIS résumé » qui ne conservent que les informations concernant le bureau d'enregistrement et l'état de l'enregistrement et ne fournissent aucune information sur le titulaire de nom de domaine. L'utilisation d'enregistrements WHOIS détaillé peut permettre une recherche de données plus rapide et plus complète lors des efforts visant à identifier les personnes malveillantes sévissant dans le DNS.

Définition de l'« efficacité »

Pour cette mesure, l'« efficacité » peut être définie par le développement d'un ensemble d'enregistrements WHOIS détaillé régulièrement utilisés par les autorités afin de suivre, d'identifier et de réduire les activités des personnes malveillantes dans le DNS.

⁶² « Politique de lutte contre les enregistrements frauduleux de .RICH », mise en ligne le 11 février 2016, <http://nic.rich/files/policies/rich-anti-abuse-policy.pdf>,

⁶³ « Politique de lutte contre les enregistrements frauduleux d'Afilias », mise en ligne le 11 février 2016, <http://dotblue.blue/about/afili-as-anti-abuse-policy>

⁶⁴ WHOIS de l'ICANN, « Guide d'initiation au WHOIS », mis en ligne le 11 février 2016, <https://whois.icann.org/en/primer>

Contexte actuel

Tous les opérateurs de registre des nouveaux gTLD qui ont fait déléguer leur(s) TLD dans la zone racine sont tenus, dans le cadre de leurs obligations contractuelles, de créer et mettre à jour des enregistrements WHOIS détaillé.

Possibles méthodes de collecte et mesure des données

Le fait d'obliger les registres des nouveaux gTLD à mettre à jour des enregistrements WHOIS détaillé avait pour but de créer un ensemble plus complet de contacts afin de permettre aux autorités de suivre les activités malveillantes et d'y mettre un terme. Obtenir des feedbacks des victimes d'abus du DNS concernant l'utilité des enregistrements WHOIS détaillé et WHOIS résumé en matière de réduction des utilisations malveillantes du DNS pourrait constituer un moyen d'évaluer l'efficacité de cette sauvegarde.

D'autres mesures potentielles pourraient venir des données générées par le système de signalement de problèmes liés à l'exactitude du WHOIS (ARS), qui est un projet en cours de développement dont le but est d'« identifier et réaliser des études sur l'exactitude de manière systématique afin d'améliorer la qualité des coordonnées au sein du WHOIS ». ⁶⁵ Les tableaux suivants tirés du rapport de phase 2 publié en décembre 2015 résument l'exactitude globale des gTLD par rapport aux exigences syntaxiques prévues par le contrat d'accréditation de bureau d'enregistrement (RAA) 2009 par mode de contact et l'exactitude globale des gTLD par rapport aux exigences en termes d'exploitabilité des données prévues par le RAA 2009 par mode de contact ⁶⁶.

Exactitude globale des gTLD par rapport aux exigences syntaxiques prévues par le RAA 2009 par mode de contact

⁶⁵ Il convient de noter que la phase 3 de l'étude n'a pas encore été menée et qu'elle se concentrera sur les « exigences en termes d'identité » qui déterminent si le contact fourni correspond à l'individu ou à l'entité responsable du domaine. Les « exigences syntaxiques » sont définies comme le format de saisie des données WHOIS. Les « exigences en termes d'exploitabilité des données » sont définies comme la capacité des contacts à résoudre et à se connecter à un utilisateur. Il convient de noter que bien que les contacts puissent être utilisables et permettre de se connecter à un utilisateur, l'ARS ne détermine pas si l'utilisateur est celui indiqué dans l'enregistrement WHOIS. Voir « Rapport du premier cycle de la phase 2 de l'ARS du WHOIS : exactitude syntaxique et exploitabilité des données », mis en ligne le 1er février 2016, <https://whois.icann.org/en/file/whois-ars-phase-2-cycle-1-report-syntax-and-operability-accuracy> et « Système de signalement de problèmes liés à l'exactitude du WHOIS (ARS) », mis en ligne le 11 février 2016, <https://whois.icann.org/en/whoisars>

⁶⁶ Ibid.

	E-mail	Téléphone	Adresse postale	TOUS les 3 exacts
Les 3 contacts sont exacts	99,1 % ± 0,2 %	83,3 % ± 0,7 %	79,4% ± 0,8%	67,2 % ± 0,9 %

Exactitude globale des gTLD par rapport aux exigences en termes d'exploitabilité des données prévues par le RAA 2009 par mode de contact

	E-mail	Téléphone	Adresse postale	TOUS les 3 exacts
Les 3 contacts sont exacts	87,1 % ± 0,7 %	74,0% ± 0,9%	98,0% ± 0,3%	64,7 % ± 0,9 %

Les trois phases de l'étude de l'ARS du WHOIS, qui portent respectivement sur la syntaxe, l'exactitude et la validité, peuvent fournir un ensemble de mesures indirectes de l'efficacité de cette sauvegarde. En théorie, les enregistrements WHOIS plus précis devraient fournir à la communauté anti-abus un outil utile pour lutter contre l'utilisation malveillante du DNS. Toutefois, il est peu probable que les personnes malveillantes ne cèdent facilement des coordonnées « précises ». Il reste à la CCT-RT de décider si « la syntaxe, l'exactitude et la validité » constituent des indicateurs adaptés de l'efficacité dans ce domaine.

Sauvegarde : centralisation de l'accès aux fichiers de zone

Contexte

Cette sauvegarde impose que les codes d'accès aux données des fichiers de zone du registre soient mis à disposition via une source centralisée, ce qui permet à la communauté anti-abus d'obtenir plus efficacement des mises à jour des nouveaux domaines au fur et à mesure de leur création au sein de chaque zone de TLD. L'objectif était d'obtenir le temps nécessaire pour prendre des mesures correctives dans les TLD rencontrant des problèmes de comportements malveillants.

Définition de l'« efficacité »

Pour cette sauvegarde, l'efficacité pourrait être définie par la capacité du service centralisé de données de zone (CZDS) à traiter les demandes d'accès aux données des fichiers de zone du registre en temps utile et de manière efficace afin de réduire au maximum les temps de réponse aux activités malveillantes.

Contexte actuel

En vertu de la spécification 4 de la section 2 du contrat de registre, les registres des nouveaux gTLD sont tenus de fournir des données de zone aux utilisateurs finaux en faisant la demande. Les rapports de l'ICANN mis à la disposition du public révèlent que plus de 3 millions de mots de passe pour l'accès au fichier de zone (ZFA) ont été

approuvés pour la seule année 2015.⁶⁷ Les conversations engagées avec les chercheurs dans le domaine de la sécurité aux fins du présent rapport indiquent que le CZDS propose un service très utile aux victimes d'abus du DNS et aux personnes souhaitant protéger leur propriété intellectuelle. Toutefois, bien que le CZDS ait été développé dans le but de renforcer l'efficacité du processus de fourniture d'accès aux fichiers de zone, les registres eux-mêmes ont fait part d'une grande frustration à l'égard du système.⁶⁸ Les opérateurs de registre doivent toujours vérifier les antécédents de l'utilisateur final et le contrat de registre ne limite pas la période au cours de laquelle les opérateurs de registre doivent répondre aux demandes d'accès. De ce fait, les demandes s'accumulent et leur gestion est bien souvent dur à assurer pour les opérateurs de registre qui ne disposent pas des capacités nécessaires pour répondre à ces demandes en temps utile. Un représentant de registre a déclaré recevoir entre 7000 et 10000 demandes d'accès au fichier de zone *par jour*.⁶⁹ Cela peut conduire à la non-application intégrale des conditions d'utilisation et à une vérification superficielle des identifiants du demandeur.⁷⁰ Pour le département de la conformité contractuelle de l'ICANN, les demandes d'accès au fichier de zone de tiers via le CZDS constituent l'un des problèmes majeurs eu égard à la conformité des registres pour l'année 2015, la plupart des plaintes ayant trait à l'incapacité des opérateurs de registre à répondre aux demandes d'accès au fichier de zone et au fait que les opérateurs de registre se voient refuser l'accès pour des motifs non prévus par le contrat de registre.⁷¹

Possibles méthodes de collecte et mesure des données

Un éventuel indicateur de l'« efficacité » pourrait résider dans les rapports du CZDS relatifs aux mots de passe qui divulguent le nombre de mots de passe de ZFA (donnés aux utilisateurs ayant demandé l'accès aux fichiers de zone en masse) au sein du CZDS ainsi que le nombre de mots de passe approuvés chaque mois au sein de TLD donnés et globalement.⁷² Les feedbacks des utilisateurs sur le service peut renforcer la crédibilité de cette mesure étant donné que de nombreux utilisateurs signalent des problèmes avec le traitement des demandes du CZDS, même s'il s'agit parfois de problèmes anecdotiques.

⁶⁷ ZFA du CZDS - Rapports mensuels relatifs aux mots de passe, mis en ligne le 1er février 2016, <https://czds.icann.org/en/reports>

⁶⁸ Opérations et politiques de recherche de l'ICANN, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 janvier 2016, délibérations de la téléconférence, enregistrements disponibles sur <https://newgtlds.icann.org/en/reviews/dns-abuse>

⁶⁹ Ibid.

⁷⁰ Ibid.

⁷¹ « Rapport annuel 2015 de l'ICANN sur la conformité contractuelle », janvier 2016, <https://www.icann.org/en/system/files/files/annual-2015-27jan16-en.pdf>

⁷² ZFA du CZDS - Rapports mensuels relatifs aux mots de passe, mis en ligne le 1er février 2016, <https://czds.icann.org/en/reports>

Sauvegarde : documentation des points de contacts et des procédures pour le signalement d'abus au niveau du registre

Contexte

Cette sauvegarde impose aux opérateurs de registre de fixer un point de contact unique chargé de la gestion des plaintes en matière d'abus. Le guide de candidature enjoint aux candidats de définir un « plan de mise en œuvre afin d'établir et de publier sur leur site Internet un point de contact unique en matière d'abus chargé de traiter les problèmes nécessitant une attention immédiate et de répondre rapidement aux plaintes signalant un abus... ». ⁷³ La spécification 6 de la section 4.1 du contrat de registre prévoit ce qui suit : « L'opérateur de registre doit fournir à l'ICANN et publier sur son site Internet ses coordonnées exactes, y compris des adresses e-mail et postale valides et le contact primaire chargé de traiter toutes les questions relatives aux problèmes de comportements malveillants dans le TLD. En outre, il informera immédiatement l'ICANN de tout changement apporté à ces coordonnées ». ⁷⁴

Définition de l'« efficacité »

Pour cette mesure, l'efficacité pourrait être mesurée selon le degré de disponibilité de ces informations à l'égard des utilisateurs finaux et en trouvant une façon de mesurer la relative facilité avec laquelle les utilisateurs peuvent signaler des cas d'abus du DNS. Une approche complémentaire consisterait à interroger les autorités chargées de l'application de la loi et les opérateurs de registre afin de connaître leurs feedbacks sur l'efficacité de cette mesure.

Contexte actuel

Le département de la conformité contractuelle de l'ICANN a assuré le suivi des informations relatives au point de contact en matière d'abus que les registres sont tenus de publier sur leur site Internet et a indiqué ce qui suit lors de la dernière mise à jour du département de la conformité contractuelle concernant cette question :

L'ICANN a continué à assurer un suivi proactif des informations relatives au point de contact en matière d'abus que les registres sont tenus de publier sur leur site Internet en vertu du nouveau contrat de registre. Ce faisant, l'ICANN veille à ce que les utilisateurs finaux, notamment les organismes chargés de l'application de la loi, trouvent un point de contact pour signaler toutes activités malveillantes dans les TLD...
L'ICANN a examiné les sites Internet de 64 domaines de premier niveau

⁷³ « Guide de candidature aux gTLD », 4 juin 2012, <https://newgtlds.icann.org/en/applicants/agb>

⁷⁴ « Contrats de registre », 9 janvier 2014, <https://www.icann.org/resources/pages/registries/registries-agreements-en>

qui ont commencé la période de revendication de marques entre le 1er janvier 2015 et le 31 mars 2015. Le nombre de demandes ou d'avis de non-conformité envoyés aux registres était inférieur à celui de la série de suivi précédente. Voici certaines des irrégularités constatées : absence d'affichage des informations requises, absence de contact primaire ou absence de l'adresse postale pour les rapports d'abus. L'ICANN collabore avec les registres afin de remédier aux irrégularités constatées.⁷⁵

Les premiers feedbacks de la communauté relatifs à cette sauvegarde indiquent que les points de contact en matière d'abus ont été principalement utilisés par les spammeurs.⁷⁶

Possibles méthodes de collecte et mesure des données

L'analyse des rapports du département de la conformité contractuelle de l'ICANN et des témoignages des personnes ayant utilisé ces contacts pourrait permettre de mesurer l'efficacité de cette sauvegarde. Une autre méthode pourrait consister à recueillir les informations relatives au point de contact en matière d'abus des registres et à tester leur fonctionnalité.

Sauvegarde : participation à un processus de requête de sécurité de registre accélérée (ESRS)

Contexte

Cette sauvegarde prévoit un mécanisme permettant aux opérateurs de registre de prendre rapidement des mesures décisives à la lumière des menaces systémiques pesant sur le DNS en définissant un processus spécial de révision et d'approbation des requêtes de sécurité accélérées. Dans la pratique, les registres sont autorisés à demander une dispense contractuelle les exemptant d'une disposition spécifique du contrat de registre pendant le délai requis pour répondre à une menace à la sécurité. Cette sauvegarde a été conçue afin de garantir la sécurité opérationnelle en cas de menace tout en tenant informées les parties concernées de l'état de la menace. Il convient de noter que ce processus a été établi en réponse au virus Conficker, avant le début des travaux visant à définir des sauvegardes pour le programme des nouveaux

⁷⁵ Voir « Mise à jour du département de la conformité contractuelle de l'ICANN - Mars 2015 », <https://www.icann.org/en/system/files/files/compliance-update-mar15-en.pdf>.

⁷⁶ Opérations et politiques de recherche de l'ICANN, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 janvier 2016, délibérations de la téléconférence, enregistrements disponibles sur <https://newgtlds.icann.org/en/reviews/dns-abuse>

gTLD. Il n'est pas inclus dans le dernier contrat de registre mais il est mis à la disposition des registres en ayant clairement besoin à un moment donné.⁷⁷

Définition de l'« efficacité »

L'« efficacité » pourrait être définie comme la rapidité avec laquelle une menace à la sécurité a été identifiée et neutralisée via l'ERSR.

Contexte actuel

De par le caractère sensible des données en jeu, l'ICANN ne communique pas publiquement les détails de ce processus. Toutefois, les premiers feedbacks des chercheurs dans le domaine de la sécurité aux fins du présent rapport indiquent que la sauvegarde a été utilisée efficacement depuis l'émergence du virus Conficker afin de démanteler les réseaux zombies en découlant.

Possibles méthodes de collecte et mesure des données

Afin de comprendre l'efficacité de cette mesure, les feedbacks des individus ayant demandé le processus ERSR pourraient être recueillis afin d'en savoir plus sur leur capacité à gérer les menaces à la sécurité. Vu la quantité limitée des demandes d'ERSR et le caractère sensible des données relatives à la sécurité inhérentes au processus, l'analyse pourrait se pencher sur *la façon* dont le processus a été mené, par exemple la rapidité et la relative facilité avec lesquelles la menace a été contrecarrée via l'ERSR, plutôt que sur le nombre de fois où le processus ERSR a été déclenché ou la façon précise dont il a été fait face à la menace à la sécurité.

Question : Comment fournir un cadre de contrôle amélioré pour les TLD avec un potentiel intrinsèque de comportements malveillants ?

Sauvegarde : créer un projet de cadre pour un programme de vérification des zones de haute sécurité

Contexte

Cette *recommandation*, qui n'a jamais été formellement prévue dans le contrat de registre en tant que sauvegarde requise ni instituée en tant qu'initiative soutenue par l'ICANN, suggérait de créer un programme volontaire pour les opérateurs de registre souhaitant renforcer le niveau de sécurité et de confiance dans leur TLD. L'objectif global du programme était de fournir un ensemble normalisé de pratiques pour les registres souhaitant se démarquer dans ce sens.⁷⁸

⁷⁷ « Rapport final du groupe de travail sur les politiques en matière d'enregistrements frauduleux », mai 2010, <http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf>

⁷⁸ icann.org, « Consultation publique : Rapport final sur les TLD de zone de haute sécurité », 11 mars 2011, <https://www.icann.org/news/announcement-2011-03-11-en>

Définition de l'« efficacité »

Pour cette mesure, l'« efficacité » pourrait être envisagée comme la réussite de l'adoption, de la mise en œuvre et de la vérification d'une zone de haute sécurité (HSZ) dans un TLD avec un fort potentiel d'activités malveillantes (par exemple les TLD représentant le secteur bancaire/financier et pharmaceutique).

Contexte actuel

Bien qu'aucun projet de cadre pour un tel programme n'ait été formalisé via les différents mécanismes d'élaboration et de mise en œuvre de politiques de l'ICANN, des initiatives ont cherché à satisfaire les besoins grandissants de certaines chaînes en matière de sécurité.

Lors du processus de candidature à un nouveau gTLD, les politiques de sécurité des candidats concernant les chaînes sensibles ont été évaluées sur la base des directives de la question 30 du guide de candidature qui imposent aux candidats de

...fournir un résumé de la politique de sécurité pour le registre proposé, incluant mais ne se limitant pas à...[a] une description de tous les niveaux de sécurité ou des capacités accrues en rapport avec la nature de la chaîne TLD faisant l'objet d'une candidature, y compris l'identification des normes de sécurité internationales ou relatives à l'industrie existantes que le candidat s'engage à suivre...⁷⁹

De plus, le Comité consultatif gouvernemental de l'ICANN a recommandé de créer un modèle pour la vérification et la validation des identifiants de l'opérateur de registre en tant qu'engagements d'intérêt public (PIC) dans des secteurs très réglementés afin d'assurer et de maintenir la fiabilité de ces domaines.⁸⁰

Un certain nombre d'activités visant à renforcer la sécurité et la confiance dans les nouveaux gTLD ont également vu le jour à l'initiative des associations de l'industrie et des registres. Par exemple, le registre fTLD Service, LLC travaille, en toute indépendance, à la création d'une zone de haute sécurité pour ses TLD « .bank » et « .insurance ». ⁸¹ Le « Projet DNS Seal » cherche lui à renforcer la confiance dans l'industrie des noms de domaine via l'autoréglementation et l'identification des

⁷⁹ « Guide de candidature aux gTLD », 4 juin 2012,

<https://newgtlds.icann.org/en/applicants/agg>

⁸⁰ Voir « Communiqué du GAC – Buenos Aires, Argentine », 24 juin 2015,

<https://www.icann.org/news/announcement-2-2015-06-24-en> et « Communiqué du GAC - Dublin, Irlande », 21 octobre 2015, <https://www.icann.org/news/announcement-2015-10-22-en>

⁸¹ Voir les services de registre fTLD, « Sécurité renforcée », mis en ligne le 11 février 2016, www.ftld.com/enhanced-security/

meilleures pratiques visant à aider les internautes à identifier les sites Web de confiance.⁸²

Possibles méthodes de collecte et mesure des données

La collecte des données des opérateurs de registre expliquant pourquoi ils ont choisi de ne pas procéder à une vérification de la HSZ pourrait faire comprendre l'absence d'adoption de cette sauvegarde recommandée. De même, le fait d'engager des discussions avec le registre fTLD Service, LLC sur les raisons pour lesquelles il a choisi de ne pas procéder à une vérification de sa propre HSZ pourrait apporter des données supplémentaires.

Proposition et modèles de recherche

D'importantes reconstitutions empiriques sont en jeu eu égard à la relation entre le développement du DNS via le programme des nouveaux gTLD et la prévalence de comportements abusifs criminels dans le DNS. D'importantes questions subsistent quant au fait de savoir si le programme des nouveaux gTLD a favorisé une augmentation des utilisations malveillantes du DNS *proportionnelle à l'augmentation de la taille du DNS découlant du programme* et, question fondamentale, **si les sauvegardes mises en place afin de réduire ces utilisations malveillantes ont permis d'atteindre leurs objectifs affichés**. Toutefois, le corpus d'ouvrages portant sur l'utilisation malveillante du DNS comprend presque exclusivement des études reposant sur des données statistiques descriptives et des enquêtes spécifiques sur les activités malveillantes sévissant au sein du DNS, et manque clairement d'études longitudinales à portée générale ayant recours à des analyses statistiques multivariées et inférentielles.

Afin d'avoir une vision globale de la situation des utilisations malveillantes du DNS dans les nouveaux gTLD et afin d'évaluer l'efficacité des sauvegardes en termes de réduction de ces utilisations malveillantes, ce rapport propose une analyse causale fondée sur des hypothèses et qui utilise les sauvegardes en tant que variables intervenant dans un ensemble de modèles hypothétiques construits sur la base de suppositions raisonnables relatives à la relation entre le programme des nouveaux gTLD et la prévalence des comportements malveillants dans le DNS. Le modèle s'attache à répondre à une question de base :

Dans quelle mesure les sauvegardes mises en place afin d'atténuer l'utilisation malveillante du DNS dans les nouveaux gTLD expliquent la proportion des comportements malveillants dans le DNS ?

⁸² « À propos du Projet DNS Seal », mis en ligne le 12 février 2016, http://dnsseal.wiki/About_the_DNS_Seal_Project

Répondre à cette question de manière complète, scientifique et sensée implique de construire un modèle hypothétique testable et de segmenter les recherches afin de se concentrer sur les TLD historiques et/ou les nouveaux TLD et/ou l'ensemble de l'espace du DNS, selon les besoins. Cela implique d'établir une **mesure de référence** en tant que point de départ à la réponse à la question de base visant à savoir s'il y a eu une augmentation des utilisations malveillantes du DNS suite au lancement du programme des nouveaux gTLD *proportionnelle au développement du DNS même*. Une fois cette mesure établie, nous pouvons commencer à poser des **questions sur les taux d'abus avant et après la mise en place des sauvegardes dans le cadre du développement du DNS**. Cela permet aux chercheurs de contextualiser l'éventuelle relation entre les neuf sauvegardes et le taux actuel d'abus du DNS.⁸³

Les modèles ci-dessous peuvent se voir appliquer des méthodes de test aussi bien qualitatives que quantitatives. Toutefois, comme vu précédemment, bon nombre des mesures de sauvegarde ne génèrent pas suffisamment de données quantitatives afin de pouvoir mener une analyse statistique solide. Deux approches peuvent résoudre ce problème : envisager de recourir à des mesures indirectes de l'efficacité des sauvegardes et utiliser des méthodes qualitatives, par exemple des entretiens avec des internautes, des groupes de discussion, l'examen de publications d'intérêt, afin de renforcer la dimension empirique au-delà du choix des méthodes quantitatives dans le contexte des sauvegardes.

Possible cadre qualitatif pour tester l'efficacité des sauvegardes

La proposition et les modèles ci-dessous constituent les premières étapes permettant d'éclairer les discussions sur les moyens les plus efficaces de tester l'efficacité des sauvegardes visant à atténuer l'utilisation malveillante du DNS. Il reste à la CCT-RT de décider de la portée et de la méthode de son enquête sur les initiatives d'atténuation des utilisations malveillantes du DNS.

Plan de registre : questions et considérations clés

Il existe un nombre incalculable de données potentielles, qualitatives et quantitatives, qui pourraient éventuellement être utilisées afin d'enquêter sur l'efficacité des neuf sauvegardes visant à atténuer les utilisations malveillantes du DNS. Toutefois, avant

⁸³ Il convient de noter que cette approche visant à comparer le taux d'abus dans les gTLD historiques actuel et avant le lancement du programme des nouveaux gTLD au taux d'abus dans les nouveaux gTLD a été avancée et préconisée par un certain nombre de participants à la téléconférence consacrée à la mesure des utilisations malveillantes du DNS et à l'efficacité des neuf sauvegardes. Voir Opérations et politiques de recherche de l'ICANN, "Reviewing New gTLD Program Safeguards Against DNS Abuse," 28 janvier 2016, délibérations de la téléconférence, enregistrements disponibles sur <https://newgtlds.icann.org/en/reviews/dns-abuse>

de décider quelles données utiliser, un plan de recherche doit être défini afin de structurer les données et d'atteindre les objectifs en termes d'examen. Le plan de recherche doit satisfaire les critères suivants :⁸⁴

1. Identifier précisément le problème de recherche. À quelle reconstitution empirique souhaitons-nous procéder ?
2. Examiner et résumer les publications déjà parues concernant le problème posé.
3. Détailler le plus possible les questions et/ou hypothèses de recherche essentiels au problème de recherche.
4. Bien décrire les données nécessaires afin de répondre correctement aux questions de recherche et/ou afin de tester les hypothèses, et expliquer comment ces données seront obtenues.
5. Décrire les méthodes d'analyse des données afin de déterminer si les hypothèses se vérifient ou non.

Les questions/réponses ci-dessous contextualisent ces tâches de recherche associées à l'examen de l'utilisation malveillante du DNS :

1. Identifier précisément le problème de recherche. À quelle reconstitution empirique souhaitons-nous procéder ?

Problème de recherche : On ignore la mesure dans laquelle les sauvegardes visant à atténuer les utilisations malveillantes du DNS dans les nouveaux gTLD ont été efficaces.

Reconstitution empirique : Certains indicateurs laissent penser que de manière générale le nombre d'abus du DNS dans les TLD (nouveaux et historiques) a été réduit alors que d'autres mettent en évidence une augmentation des abus dans certains TLD. La mesure dans laquelle les sauvegardes visant à atténuer les utilisations malveillantes du DNS ont joué un rôle dans cette évolution reste obscure.

2. Examiner et résumer les publications déjà parues concernant le problème posé.

Le présent rapport a pour but d'assurer cet examen et de faire ce résumé.

3. Détailler le plus possible les questions et/ou hypothèses de recherche essentiels au problème de recherche.

⁸⁴ Ces critères ont été tirés d'une liste succincte de questions de recherche de l'université de Californie du Sud disponible sur <http://libguides.usc.edu/writingguide/researchdesigns> (mise en ligne le 26 février 2016).

Question(s) de recherche : Qu'est-ce qui explique l'évolution des taux d'abus dans les différents TLD ? Dans quelle mesure les sauvegardes mises en place afin de réduire ces abus ont-elles été efficaces ?

Exemples hypothétiques (voir les modèles ci-dessous pour une analyse plus approfondie de la définition des relations hypothétiques) :

- Niveau supérieur (pour orienter l'ensemble ou une partie significative de l'examen) :
 - Le développement du DNS a engendré une *augmentation* du nombre d'utilisations malveillantes du DNS qui n'est pas proportionnelle avec ledit développement.
- Niveau inférieur (pour orienter des parties précises de l'enquête dans le cadre de l'examen) :
 - La sauvegarde X, qui tentait de prévenir la forme d'utilisation malveillante du DNS Y, n'a pas réussi à atteindre ses objectifs.

Les questions de recherche et hypothèses devraient également indiquer la façon dont chaque terme est défini et/ou mesuré. Par exemple, comme vu précédemment, comment mesurer l'« efficacité » d'une sauvegarde ?

4. Bien décrire les données nécessaires afin de répondre correctement aux questions de recherche et/ou afin de tester les hypothèses, et expliquer comment ces données seront obtenues.

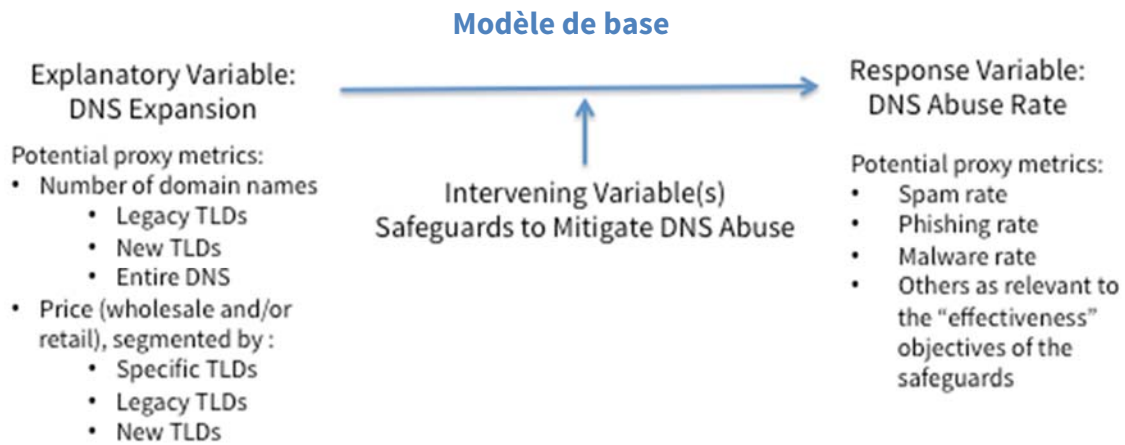
Par exemple, l'« efficacité » des sauvegardes peut être mesurée qualitativement via des entretiens menés auprès d'experts et d'utilisateurs des sauvegardes. La mesure dans laquelle le programme des nouveaux gTLD a contribué à l'utilisation malveillante du DNS pourrait être mesurée quantitativement en examinant les corrélations statistiques entre le nombre de nouveaux domaines et un indicateur d'abus du DNS, par exemple le taux d'hameçonnage.

5. Décrire les méthodes d'analyse des données afin de déterminer si les hypothèses se vérifient ou non.

À déterminer par les travaux de la CCT-RT en plus de la définition des questions de recherche et hypothèses tel que vu précédemment.

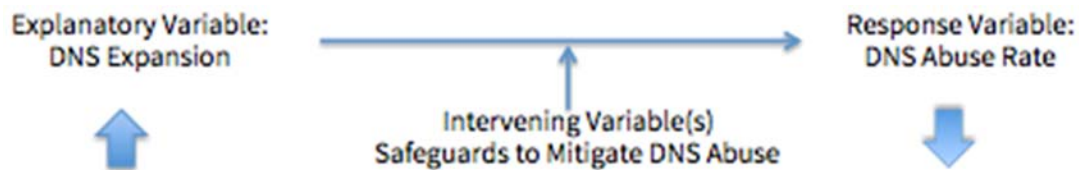
Modèles causaux et hypothèses

Les modèles susmentionnés découlent d'une simple hypothèse de base selon laquelle, du moins en théorie, l'introduction des sauvegardes visant à prévenir toute utilisation malveillante du DNS dans les nouveaux gTLD devraient conduire à un espace de DNS « plus propre » (c'est-à-dire avec moins d'activités malveillantes) par rapport à l'époque des TLD historiques où de telles sauvegardes n'existaient pas.



Trois scénarios hypothétiques testables découlent de ce modèle de base :

Modèle 1 : Le développement du DNS a entraîné une *baisse* proportionnelle des utilisations malveillantes du DNS (hypothèse de sauvegarde efficace)

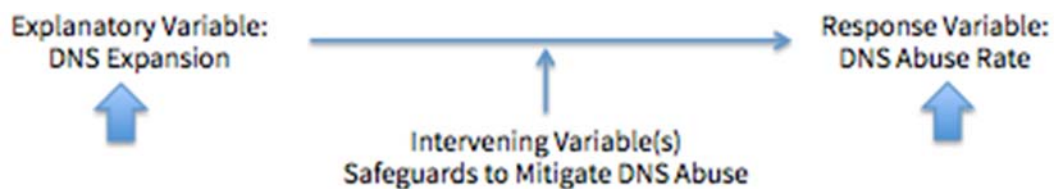


Question de recherche : Dans quelle mesure des sauvegardes efficaces sont-elles des facteurs de causalité expliquant la *baisse* proportionnelle des utilisations malveillantes du DNS ?

Hypothèse 1 : Le développement du DNS « sauvegardé » est un facteur de causalité expliquant la **baisse** proportionnelle des utilisations malveillantes du DNS dans les TLD historiques et/ou nouveaux et/ou dans l'ensemble du DNS (analyse segmentée par TLD nouveau et/ou historique et/ou pour l'ensemble du DNS, selon le cas).

Hypothèse 1.1 : Les sauvegardes mises en place afin d'atténuer les utilisations malveillantes du DNS **ont permis** d'atteindre les objectifs affichés et sont des facteurs de causalité expliquant la baisse proportionnelle des utilisations malveillantes du DNS (analyse des sauvegardes individuelles cibles si besoin est).

Modèle 2 : Le développement du DNS via le programme des nouveaux gTLD a conduit à une *augmentation* proportionnelle des utilisations malveillantes du DNS.
(hypothèse de sauvegarde inefficace)

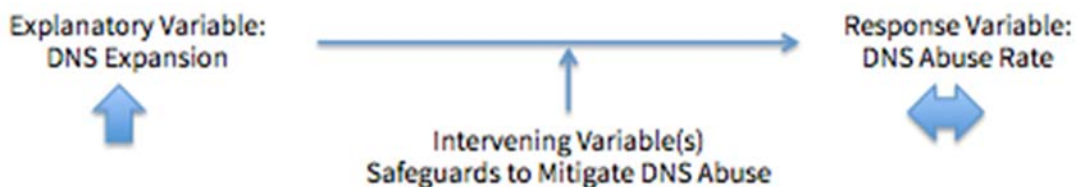


Question de recherche : Dans quelle mesure des sauvegardes inefficaces sont-elles des facteurs de causalité expliquant l'*augmentation* proportionnelle des utilisations malveillantes du DNS ?

Hypothèse 2 : Le développement du DNS « sauvegardé » est un facteur de causalité expliquant l'**augmentation** proportionnelle des utilisations malveillantes du DNS dans les TLD historiques et/ou nouveaux et/ou dans l'ensemble du DNS (analyse segmentée par TLD nouveau et/ou historique et/ou pour l'ensemble du DNS, selon le cas).

Hypothèse 2.1 : Les sauvegardes mises en place afin d'atténuer les utilisations malveillantes du DNS **n'ont pas permis** d'atteindre les objectifs affichés (analyse des sauvegardes individuelles cibles si besoin est).

Modèle 3 : Le développement du DNS n'a eu *aucun effet* sur l'utilisation malveillante du DNS.
(hypothèse de sauvegarde inefficace)



Question de recherche : Dans quelle mesure des sauvegardes inefficaces sont-elles des facteurs de causalité expliquant le *statu quo* des utilisations malveillantes du DNS ?

Hypothèse 3 : Le développement du DNS « sauvegardé » n'a eu aucun effet sur la proportion des comportements malveillants survenus dans les TLD historiques et/ou nouveaux et/ou dans l'ensemble du DNS (analyse segmentée par TLD nouveau et/ou historique et/ou pour l'ensemble du DNS, selon le cas).

Hypothèse 3.1 : Les sauvegardes mises en place afin d'atténuer les utilisations malveillantes du DNS **n'ont pas permis** d'atteindre les objectifs affichés de fourniture d'un espace de nouveaux gTLD plus « sûr » par rapport à l'espace historique (analyse des sauvegardes individuelles cibles si besoin est).

En ce qui concerne les travaux de la CCT-RT, cette proposition de recherche constitue une possible approche de structuration de son enquête sur la capacité des neuf sauvegardes à atténuer les utilisations malveillantes du DNS. Une telle approche impliquera probablement de faire appel à des fournisseurs externes capables de procéder à un recueil et à une analyse des données statistiques et qualitatives afin de construire et de mener l'étude actuelle. Il reste à la CCT-RT de décider de la portée et de la méthode de l'analyse qui sera menée. Cette proposition de recherche peut au moins servir de base à des discussions sur d'autres approches éventuelles.

Annexe : Étude sur les activités liées aux utilisations malveillantes au sein de l'ICANN

Projet	Portée	Source et liens
Spécification 11 du contrat de registre	<p><u>Section 3a</u> : « L'opérateur de registre inclura dans son contrat registre/bureau d'enregistrement une disposition en vertu de laquelle les bureaux d'enregistrement doivent inclure dans leurs contrats d'enregistrement une disposition interdisant aux détenteurs de domaines enregistrés 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) les sanctions pour ce type d'activités, y compris la suspension du nom de domaine. »</p> <p><u>Section 3b</u> : « L'opérateur de registre procédera périodiquement à une analyse technique afin d'évaluer si les domaines de son TLD sont utilisés de façon à perpétrer des menaces à la sécurité comme le dévoiement, le hameçonnage, les programmes malveillants et les réseaux zombies. L'opérateur de registre rédigera des rapports statistiques sur le nombre des menaces à la sécurité identifiées et les mesures prises suite aux vérifications périodiques en matière de sécurité. L'opérateur de registre rédigera ces rapports pendant la durée du contrat, sauf si un délai plus court est requis par la loi ou approuvé par l'ICANN, et il les présentera à l'ICANN sur demande. »</p>	<p>Source : Contrat de registre</p> <p>Lien : Contrats de registre</p> <p>Lien : FAQ : Spécification 11 du contrat de registre pour les nouveaux gTLD révisé</p>
Recommandation 11 de l'équipe de révision SSR	<u>Recommandation 11</u> : « L'ICANN devrait définir et mettre en place des actions visant à mesurer le succès des nouveaux gTLD et des procédures accélérées IDN	Source : équipe de révision de la sécurité, la stabilité et la résilience du DNS

	<p>qui soient expressément en rapport avec les objectifs en matière de SSR, y compris des mesures de l'efficacité des mécanismes destinés à atténuer l'utilisation malveillante des noms de domaine. »</p>	<p>Lien : Rapport final de l'équipe de révision de la sécurité, la stabilité et la résilience du DNS</p>
<p>Avis du GAC : ICANN53 et ICANN54</p>	<p><u>Communiqué de Buenos Aires de l'ICANN53</u> : « Le GAC...recommande...à la communauté de l'ICANN d'élaborer une méthodologie harmonisée pour compter le nombre d'enregistrements abusifs de noms de domaine dans le cadre de l'évaluation en cours du programme des nouveaux gTLD. »</p> <p><u>Communiqué de Dublin de l'ICANN54</u> : « Le GAC recommande au Conseil d'administration et l'exhorte à...élaborer et adopter une méthodologie harmonisée visant à communiquer à la communauté de l'ICANN les niveaux et la persistance des comportements malveillants (par exemple programmes malveillants, réseaux zombies, hameçonnage, dévoiement, piraterie, violation de marques ou de propriété intellectuelle, contrefaçons, pratiques frauduleuses ou nuisibles et autres activités illégales) survenus lors du déploiement du programmes des nouveaux gTLD. »</p>	<p>Source : Comité consultatif gouvernemental de l'ICANN</p> <p>Lien : Communiqué du GAC de l'ICANN53, Buenos Aires</p> <p>Lien : Communiqué du GAC de l'ICANN54, Dublin</p>
<p>Avis du SSAC sur la protection des titulaires de noms de domaine : meilleures pratiques pour préserver la sécurité et la stabilité dans le cycle de gestion des informations d'identification</p>	<p><u>Recommandation 1</u> : « Dans le cadre de ses rapports périodiques, le département de la conformité contractuelle de l'ICANN devrait publier des données sur les atteintes à la sécurité que les bureaux d'enregistrement ont signalées conformément au paragraphe 3.20 du contrat d'accréditation de bureau d'enregistrement 2013 (RAA). »</p> <p><u>Recommandation 2</u> : « Une disposition analogue au paragraphe 3.20 du RAA 2013 devrait être incorporée dans tous les futurs contrats de registre et des données statistiques similaires devraient être publiées conformément à la recommandation 1 ci-dessus. »</p>	<p>Source : Comité consultatif sur la sécurité et la stabilité</p> <p>Lien : Avis SAC074</p>

<p>Indice santé pour le marché des gTLD</p>	<p>L'ICANN a développé un ensemble de concepts potentiels à discuter avec la communauté afin d'apporter un éclairage sur la création de son indice santé pour le marché des gTLD, concepts axés sur (i) une forte concurrence, (ii) la confiance du consommateur et (iii) la stabilité non technique.</p> <p>Cette proposition de concepts vise à faciliter les échanges au sein de la communauté concernant ce qu'on entend par « bonne santé » du marché mondial des gTLD. Ces discussions au sein de la communauté sont censées générer des facteurs mesurables faisant office d'indicateurs clés de performance pour le marché des gTLD.</p> <p>Un certain nombre de concepts portent sur l'utilisation malveillante du DNS comme décrit dans le présent rapport.</p>	<p>Source : personnel de l'ICANN</p> <p>Lien : Proposition de création d'un indice santé pour le marché des gTLD : appel à commentaires et à volontaires</p>
---	---	--