Nouveau programme gTLD
Mémorandum explicatif

Réduction des comportements malveillants

Date de publication : 3 Octobre 2009

Origines - Nouveau programme gTLD

Depuis la création de l'ICANN il y a dix ans comme organisme multipartie sans but lucratif, chargé de coordonner le système d'adressage de l'Internet, l'un de ses principes fondamentaux, reconnu par les États-Unis et d'autres gouvernements, a été de promouvoir la concurrence dans le marché des noms de domaine tout en assurant la sécurité d'Internet et sa stabilité. L'expansion de domaines génériques de premier niveau (gTLD) permettra davantage d'innovation, de choix et de changement du système d'adressage Internet, représenté aujourd'hui par 21 gTLD.

La décision d'introduire de nouveaux TLD génériques a suivi une procédure de consultation longue et détaillée avec toutes les parties prenantes de la communauté Internet mondiale représentées par une grande variété d'intervenants – gouvernements, individus, sociétés civiles, les entreprises et les circonscriptions de propriété intellectuelle, et la communauté technologique. Ont également contribué : le Comité consultatif gouvernemental de l'ICANN (GAC), le Comité consultatif At-Large (ALAC), Country Code Names Supporting Organization (ccNSO), et le Comité consultatif de la sécurité et la stabilité (SSAC). Le processus de consultation a abouti à une politique sur l'introduction de nouveaux gTLD complété par la Generic Names Supporting Organization (GNSO) en 2007, et adopté par le conseil de l'ICANN en Juin 2008. Le programme est prévu pour un lancement dans l'année civile 2010.

Ce mémorandum explicatif fait partie d'une série de documents publiés par l'ICANN pour aider la communauté mondiale de l'Internet dans la compréhension des exigences et des processus présentés dans le Guide du demandeur, qui est actuellement sous forme de projet. Depuis la fin de 2008, le personnel de l'ICANN a partagé les progrès du développement du programme avec la communauté Internet à travers une série de forums de discussion publique sur les projets guide du demandeur et des documents secondaires. À ce jour, il y a eu plus de 250 journées de consultation sur les matériaux critiques du programme. Les commentaires reçus continuent à être soigneusement évalués et utilisés pour affiner le programme et éclairer l'élaboration de la version finale du guide du demandeur.

Pour une mise à jour des informations, échéances et activités liées au Programme des nouveaux gTLD, veuillez consulter http://www.icann.org/en/topics/new-gtld-program.htm.

Veuillez prendre note qu'il s'agit d'un projet de discussion. Les candidats éventuels ne devraient pas se fier à aucun des détails du programme proposé pour les nouveaux gTLD tant que ce programme reste en cours de consultation et de révision.

Résumé des points clés de ce document

L'ICANN sollicite des observations sur la proposition visant à ajouter des mesures spécifiques pour l'accord du nouveau registre TLD générique, décrit ci-dessous, qui est exigé de tous les registres afin de réduire le comportement malveillant potentiel.

Au cours de l'étude des comportements malveillants, le personnel de l'ICANN a demandé et reçu des commentaires provenant de plusieurs sources extérieures, incluant le Groupe de travail Anti Hameçonnage (APWG), le Registre Internet Groupe de Sécurité (RISG), le Comité consultatif de la sécurité et la stabilité (SSAC), le Computer Emergency Response Teams (CERT) et les membres en sécurité financière / bancaire, et les collectivités d'Internet. Ces parties ont décrit les problèmes potentiels de plusieurs comportements malveillants et ont encouragé l'ICANN à examiner les moyens qui pourraient être utilisés dans les accords du nouveau registre gTLD. Ces mesures recommandées ont pour but d'accroître les avantages pour la sécurité globale et la stabilité pour les déclarants, et la confiance de tous les utilisateurs de ces zones de nouveaux gTLD.

Les commentaires reçus sur la version 2 du Projet de Guide du Demandeur, au cours de la réunion de Sydney et dans les consultations depuis Sydney ont recommandé des mesures et des contrôles destinés à réduire les comportements malveillants, doivent être intégrés comme obligatoires dans le projet d'accord de base de registre pour les nouveaux gTLD. Ce qui suit est un résumé des contributions considérées et de la procédure suivie dans la préparation de ces recommandations.

Les recommandations fournissent des mesures de réduction concrètes des risques de comportement malveillant dans neuf domaines :

1. Opérateurs de registre confirmés
2. Plan démontré pour le déploiement DNSSEC
3. Interdiction du wildcarding
4. Suppression des fichiers orphelins quand une entrée de nom de serveur est supprimée de la zone
5. Nécessité d'étoffer les fichiers Whois
6. Centralisation des accès aux fichiers de zone
7. Contacts et procédures documentées du taux d'abus du registre
8. Participation à un processus de Demande de Sécurité de Registre Accéléré
9. Projet de structure pour la vérification des zones de haute sécurité

Ensemble, nous croyons que ces mesures contribueront grandement à atténuer le risque croissant du comportement malveillant résultant de nouveaux gTLD. Le travail de la politique de ces questions et des mesures prises pour réduire les comportements malveillants vont continuer. L'ICANN peut également étudier la

formation d'un groupe de travail associant des membres de l'industrie de la sécurité et la communauté de l'ICANN, pour aider à élaborer et évaluer les solutions et implémentations spécifiques de mesures de réduction proposées.

Préface

Depuis la création de l'ICANN il y a dix ans comme organisme multipartie sans but lucratif, chargé de coordonner le système d'adressage de l'Internet, l'un de ses principes fondamentaux, reconnu par les États-Unis et d'autres gouvernements, a été de promouvoir la concurrence dans le marché des noms de domaine tout en assurant la sécurité d'Internet et sa stabilité. L'expansion va engendrer l'innovation, le choix et un changement positif pour le système d'adressage de l'Internet. Dans un monde comptant 1,5 milliard d'utilisateurs d'Internet les plus divers, le choix et la concurrence sont la clé du succès continu et à la portée du réseau mondial.

La décision de lancer ces séries de nouveaux gTLD a suivi une procédure détaillée et de longues consultations avec toutes les parties prenantes de la communauté Internet mondiale. Des représentants d'une grande variété d'intervenants— gouvernements, individus, société civile, entreprises et circonscriptions de propriété intellectuelle, et la communauté technologique — ont été engagés dans des discussions pendant plus de 18 mois. En Octobre 2007, la Generic Names Supporting Organization (GNSO)- l'un des groupes qui coordonnent la politique mondiale de l'Internet à l'ICANN — a achevé ses travaux d'élaboration de politiques sur les nouveaux gTLD et a approuvé une série de recommandations. Le point culminant du processus de développement de cette politique a été une décision prise par le conseil d'administration de l'ICANN d'adopter la politique développée par la communauté en Juin 2008 à la réunion de l'ICANN à Paris. Un mémoire complet du processus de la politique et des résultats peut être consulté à http://gnso.icann.org/issues/new-gtlds/.

Ce document fait partie d'une série de documents qui serviront de notes explicatives publiées par l'ICANN pour aider la communauté de l'Internet à mieux comprendre la demande de proposition (DP), également connue en tant que Guide du Demandeur. Une étape de commentaires publics pour le Guide du Demandeur et ces documents renseigneront une revue détaillée et l'adaptation de ces idées. Ces observations seront utilisées pour réviser les documents en préparation d'un guide final du Demandeur.

Veuillez prendre note qu'il s'agit d'un projet de discussion. Les candidats éventuels ne devraient pas se fier à aucun des détails du programme proposé pour les nouveaux gTLD tant que ce programme reste en cours de consultation et de révision.

Contribution de la communauté sur le problème de malveillance

L'ICANN a reçu de nombreux commentaires du public couvrant de multiples domaines, en réponse à son annonce proposant une expansion de l'espace TLD à déléguer aux nouveaux TLD, y compris les TLD IDN. Un des problèmes identifiés par plusieurs parties concernait le potentiel d'accroissement de comportement malveillant qui pourrait survenir de nouveaux gTLD. Afin de faire face à ce problème, l'ICANN a sollicité les commentaires des experts pour répondre aux comportements malveillants, et des intervenants touchés par le comportement malveillant dans les gTLD existants.

Les contributions reçues sur les versions antérieures 1 et 2 du Projet de Guide du Demandeur ont constitué une source primaire importante dans l'élaboration des recommandations inclues dans la version 3 du Projet de Guide du Demandeur.

Une deuxième source de contribution sur cette question est le corps des rapports émis par le SSAC sur des formes de comportement malveillant. Plus précisément, SAC038 :

Point de Contact des Registraire en cas d'abus (pdf) et SAC040 : Mesures pour protéger les services d'enregistrement de noms de domaine contre l'exploitation et le mauvais usage (pdf). Ces rapports, ainsi que d'autres travaux effectués par le SSAC, fournissent une assistance concernant les meilleures pratiques de sécurité pour les registres et registraires qui ont guidé les modifications proposées dans le Projet de Guide du Demandeur et le nouvel accord de registre gTLD.

Une troisième source est le projet de rapport établi par l'Anti-Phishing Working Group (APWG), une association industrielle axée sur l'élimination du vol d'identité et des fraudes qui découlent au problème croissant de l'hameçonnage et d'usurpation des courriels. Ce rapport a été coordonné par le Comité de Politique d'Internet (IPC) de l'APWG, qui comprend plus de 90 membres représentant l'ensemble des membres de l'APWG. Il est à noter que de nombreux intervenants de l'ICANN, y compris les registres et registraires gTLD et ccTLD, les fournisseurs de service Internet, les propriétaires de la propriété intellectuelle et de la sécurité, et des institutions financières sont des membres de l'APWG et de l'APWG IPC, voir http://www.antiphishing.org/sponsors.html. L'IPC de l'APWG considère l'expansion prévue de TLD génériques comme étant un événement important ayant un impact potentiel sur l'e-criminalité. Le rapport APWG CIB apporte une participation globale et constructive à l'ICANN sur de nombreux problèmes concernant la conduite malveillante qui d'après le CIB de l'APWG, méritent attention et planification au cours du déploiement des nouveaux TLD génériques.

Une quatrième source de contribution a été apportée par le Groupe Sécurité des Registre d'Internet (RISG), un groupe mondial d'organisations d'Internet responsables qui travaillent collectivement pour combattre le vol d'identité sur Internet, notamment l'hameçonnage et la distribution de logiciel malveillant. Le rapport RISG (pdf) fournit une énumération de plusieurs problèmes qui résulteraient de l'augmentation du nombre de registres.

Une cinquième source d'informations reçues sur la question de comportement malveillant est une série de commentaires issus de la communauté bancaire et financière. Un ensemble d'associations de l'industrie comprenant le Programme de réduction de la fraude BITS, l'American Banking Association, le Financial Services Information Sharing and Analysis Center (**FS-ISAC**) et le Financial Services Technology Consortium (FSTC) ont apporté leur expertise. Avec leur perspective unique et une expérience de sécurisation des deux réseaux et des données sensibles, cette communauté a fourni des recommandations spécifique précieuses pour les mesures que les registres devraient mettre en œuvre, incluant l'adoption de pratiques commerciales sûres, afin d'accroître la confiance des utilisateurs et de réduire le risque de compromission par des attaques malveillantes.

Une sixième source de contribution sur les mesures visant à réduire le comportement malveillant dans les nouveaux gTLD est le travail effectué par l'équipe de recommandations de mise en œuvre (IRT). Alors que l'ICANN a identifié la protection des marques et des possibilités d'abus malveillants en tant que questions distinctes à aborder dans la création de nouveaux gTLD, un entrecroisement important existe dans les approches correctives qui sont proposées pour répondre à ces préoccupations. Le travail de l'IRT a été résumé dans la « lettre ouverte de l'IRT Présentant notre travail», datée du 29 Mai 2009. L'IRT a été formé par la circonscription de la propriété intellectuelle de l'ICANN en conformité avec la résolution du Conseil de l'ICANN du 6

Mars 2009 (link) à la demande de la communauté recherchant des solutions pour faire face aux risques potentiels pour les titulaires de marques dans la mise en œuvre de nouveaux gTLD. Le rapport fourni par l'équipe de l'IRT (pdf) reflète la diversité géographique et l'expérience de ses 18 membres et deux suppléants.

D'autres sources d'information proviennent de membres de la communauté de première réponse de la sécurité Internet. Les membres des organisations telles que le Forum mondial de la réponse aux incidents et des équipes de sécurité (FIRST), qui se compose d'équipes d'intervention d'urgence de l'ordinateur et du réseau de 180 sociétés, d'organismes gouvernementaux, d'universités et autres établissements répartis dans les Amériques, Asie, Europe et Océanie pour aider à diriger les efforts internationaux pour lutter contre la cyber-criminalité, ont fourni des conseils précieux. Diverses agences du maintien de l'ordre ont fourni une assistance en définissant les questions d'importance et suggérant des changements dans les opérations d'enregistrement qui aideraient dans la lutte contre la criminalité sur Internet.

En plus des sources déjà citées, l'ICANN a inséré des informations apportées par les participants aux consultations publiques tenues à Sydney, New York, Londres, Hong Kong et à Abu Dhabi. Ces consultations comprenaient des sessions spécifiques axées sur la question de réduction du risque de comportement malveillant et des nouveaux gTLD.

L'ICANN gère un wiki sur le site icann.org consacré aux sollicitations de solutions potentielles pour faire face au comportement malveillant dans les nouveaux gTLD. Les rapports mentionnés ci-dessus ont été affichés sur ce wiki et la participation du public à poster des commentaires a été encouragée.

Principaux enjeux identifiés

Un certain nombre de questions relatives à la possibilité de comportement malveillant ont été identifiées par cet ensemble diversifié de participants dans le processus de l'ICANN. Bien que bon nombre des questions exposent d'uniques et complexes vulnérabilités techniques et nécessitent une variété de contrôles et de considérations, elles peuvent être résumées dans les thèmes clés catégorisés ci-dessous :

A. Comment s'assurer que de mauvais acteurs ne gèrent pas de Registres ?

Des sources ont demandé que l'ICANN prenne des mesures pour réduire le risque qu'un nombre accru de registres pourraient conduire à l'entrée d'opérateurs non fiables ou de criminels dans la communauté et permettre au comportement malveillant de se produire.

B. Comment assurer l'intégrité et l'utilité des informations du Registre ?

Des sources encouragent l'ICANN de profiter de la création de nouveaux TLD génériques pour améliorer la qualité de l'enregistrement de noms de domaine et les services de résolution de nom de domaine d'une manière qui limiterait les possibilités de comportement malveillant.

C. Comment garantir un effort effectif pour lutter contre les abus identifiés ?

Étant donné que le comportement malveillant existe déjà et affecte tous les TLD, des sources ont demandé à l'ICANN de poursuivre les efforts dans la création d'améliorations de nouveaux TLD et des processus et outils disponibles pour réduire la cyber-criminalité et

les abus des systèmes d'enregistrement de domaine du DNS déjà existants.

D. Comment offrir un cadre de contrôle optimal sur les TLDs ayant un potentiel intrinsèque d'abus ?

Certains nouveaux TLD peuvent nécessiter des e-transactions de services exigeant une infrastructure hautement sécurisée (par exemple, les services financiers ou le vote électroniques) et peuvent impliquer des actifs et infrastructures critiques (tels que ceux qui supportent les infrastructures énergétiques ou de services médicaux) qui doivent bénéficier d'une protection accrue des acteurs utilisant le système des noms de domaine et ayant déjà un comportement malveillant. Des sources ont recommandé à l'ICANN de prendre des mesures pour créer un système permettant une confiance renforcée dans les opérations de ces zones.

Mesures de réduction proposées :

Afin de répondre aux questions résumées ci-dessus concernant la conduite malveillante, l'ICANN considère qu'une combinaison de mesures devrait être prise dans le cadre de la mise en place prévue de nouveaux gTLD. En plus des obligations accrues de la part de nouveaux registres gTLD dans leurs contrats avec l'ICANN, ces nouveaux registres sont encouragés à négocier des normes plus strictes avec des registraires accrédités pour les pratiques commerciales et de sécurité. Plus précisément, un registre de nouveau gTLD aura la capacité d'exiger l'application des mesures spécifiques pour réduire les comportements malveillants de la part des registraires afin d'enregistrer des labels dans leur zone.

En outre, l'ICANN continuera à travailler avec la collectivité pour compléter le développement des politiques existantes et les efforts du groupe de travail afin de prévoir des mesures de réduction qui doivent être mises en œuvre au niveau de l'interface du registraire déclarant.

Voici les catégories générales de mesures de réduction proposées pour être mises en œuvre dans la version actuelle du Projet du Guide du Demandeur:

1. Opérateurs de registre confirmés
2. Plan démontré pour le déploiement DNSSEC
3. Interdiction du wildcarding
4. Suppression des fichiers orphelins quand une entrée de nom de serveur est supprimée de la zone
5. Nécessité d'étoffer les fichiers Whois
6. Centralisation des accès aux fichiers de zone
7. Contacts et procédures documentées du taux d'abus du registre
8. Participation à un processus de Demande de Sécurité de Registre Accéléré
9. Projet de structure pour la vérification des zones de haute sécurité

Relations entre les mesures de réduction des problèmes

A. Comment s'assurer que des Registres ne soient pas gérés par de mauvais acteurs ?

1. Confirmer les opérateurs de registre

B. Comment assurer l'intégrité et l'utilité des informations du Registre ?

2. Exiger le déploiement DNSSEC
3. Interdire le wildcarding
4. Encourager la suppression des enregistrements orphelins

C. Comment assurer plus d'efforts focalisés sur la lutte contre les abus identifiés ?

5. Exiger un WHOIS étoffé
6. Centraliser les accès aux fichiers de zone
7. Documenter les contacts et politiques de niveaux d'abus des Registres et registraires
8. Disponibilité du processus de Demande de Sécurité de Registre Accéléré

D. Comment offrir un cadre de contrôle accrue sur les TLDs ayant un potentiel intrinsèque de comportement malveillant ?

9. Programme de vérification des zones de haute sécurité

Mesures spécifiques à mettre en œuvre dans les nouveaux contrats de registre

Les mesures suivantes sont incluses dans le Guide du demandeur et reflètent les procédures exigées pour tous les nouveaux registres. L'emplacement de la formule dans le projet de guide du demandeur est identifié. Une brève description de la justification de chaque mesure spécifique est inclue (en italique).

1. Opérateurs de Registres confirmés

Une question au demandeur (annexe du module 2) stipule :

L'ICANN peut refuser la demande par ailleurs qualifiée pour l'une des raisons suivantes :

Le demandeur, ou tout associé, directeur, administrateur ou dirigeant, ou toute personne ou entité appartenant pour (ou véritable propriétaire) quinze pour cent ou plus du demandeur :

a. au cours des dix dernières années, a été reconnu coupable d'un crime ou d'un délit lié aux activités de gestion financière ou morale, ou a été jugé par un tribunal pour avoir commis une fraude ou manquement à une obligation fiduciaire, ou a fait l'objet d'une mesure judiciaire que l'ICANN a considéré comme l'équivalent des éléments ci-dessus;

b. au cours des dix dernières années, a été sanctionné par un gouvernement ou organisme de réglementation de l'industrie pour un comportement impliquant

la malhonnêteté ou la mauvaise utilisation des fonds d'autrui;

c. est actuellement impliqué dans une procédure judiciaire ou réglementaire qui pourrait aboutir à une condamnation, un jugement, ou une mesure disciplinaire du type indiqué en (a) ou (b);

d. fait l'objet d'une disqualification imposée par l'ICANN et en vigueur au moment où la demande est examinée ; ou

e. omet de produire à l'ICANN les informations d'identification nécessaires pour confirmer l'identité au moment de la demande

f. fait l'objet d'une convention impliquant sa responsabilité ou la pratique répétée de mauvaise foi à l'égard de l'enregistrement de noms de domaine, y compris :

(i) l'acquisition de noms de domaine essentiellement aux fins de vente, location ou de transfert des enregistrements de noms de domaine au titulaire d'une marque ou marque de service ou à un concurrent, à titre onéreux, au-delà de coût décaissé documenté relié directement au nom de domaine ; ou

(ii) l'enregistrement des noms de domaine en vue d'empêcher le propriétaire de la marque ou marque de service de reprendre sa marque dans un nom de domaine correspondant ; ou

(iii) l'enregistrement des noms de domaine essentiellement en vue de perturber les opérations commerciales d'un concurrent ; ou

(iv) l'utilisation des noms de domaine avec l'intention d'attirer, à des fins lucratives, les utilisateurs d'Internet vers un site Web ou autre espace en ligne, en créant une probabilité de confusion avec une marque ou une marque de service quant à la source, le commanditaire, l'affiliation ou l'aval du site Web ou d'un emplacement ou d'un produit ou service sur le site Web ou la location.

Note: L'information recueillie au cours de ces vérifications des antécédents incluant les données relatives aux activités criminelles antérieures seront examinées lors du processus de demande.

Le processus de demande comprendra des vérifications approfondies normalisées des antécédents et des vérifications de références pour les entreprises et les particuliers (par exemple, les agents clés). Cette étape permettra de réduire le risque que des criminels connus, membres d'organisations criminelles, ou ceux ayant des antécédents de malhonnêteté soient impliqués dans les opérations d'enregistrement ou deviennent propriétaires ou contrôle-proxy de registres.

2. Exiger le déploiement DNSSEC

Les opérateurs de registres seront tenus de fournir un plan documenté pour signer leurs fichiers de zone et avoir mis en place la mise en œuvre DNSSEC au début des opérations.

La formulation suivante a été ajoutée à la norme 6 de la version 3 de l'Accord de registre, sous réserve d'examen technique :

"L'opérateur de registres doit appliquer les extensions de sécurité des systèmes de noms

de domaines (DNSSEC). Pendant la durée, l'opérateur de registre doit se conformer aux RFC 4033, 4034, 4035, 4509 et 4310 et leurs successeurs, et suivre les meilleures pratiques décrites dans la RFC 4641 et ses successeurs. Si l'opérateur de registre met en œuvre le déni d'existence authentifié haché pour les extensions de sécurité du DNS, il doit se conformer à la norme RFC 5155 et ses successeurs. L'opérateur de registre doit accepter des documents clé publics à partir de noms de domaine enfant de façon sécurisée selon les meilleures pratiques du secteur. Le registre doit également publier sur son site Internet les mentions légales (aussi connues comme politique DNSSEC ou DPS) décrivant le stockage des clés, les accès et l'usage de ses propres clés, et le matériel trust anchor du demandeur."

Les avantages apportés par la mise en œuvre du DNSSEC à la sécurité globale et la stabilité de l'Internet sont bien documentés. L'ICANN s'est engagé à la signature de la zone racine avant la fin de l'année 2009 et fera en sorte que la création de nouveaux gTLD permette l'utilisation de cet important moyen pour améliorer la sécurité du DNS.

3. Interdiction du Wild Carding

Le rapport SAC041 par le SSAC (approuvé par le conseil de l'ICANN) et les rapports d'autres organisations ont fait savoir a l'ICANN que les nouveaux TLD ne devraient pas être autorisés à utiliser la redirection DNS et les réponses DNS synthétisées.

Compte tenu de la tendance actuelle des logiciels malveillants associés aux sites publicitaires, la redirection de domaines vers des sites de publicité présente un risque supplémentaire de comportement malveillant. Pour les noms de domaine qui soit ne sont pas enregistrés par un demandeur ou le demandeur n'a pas fourni des enregistrements valides tels que des enregistrements NS pour inscription dans le fichier de zone DNS, ou leur statut ne leur permet pas d'être publiés dans le DNS, l'utilisation d'enregistrements de ressources DNS wildcard tels que décrits dans la RFC 4592 ou toute autre méthode ou technologie pour synthétiser les enregistrements des ressources DNS ou en utilisant la redirection dans le DNS par le registre, est interdite. Plus précisément, lorsqu'ils sont interrogés pour de tels noms de domaine, les serveurs de noms faisant autorité doivent répondre par "Erreur de Nom" (également connu sous le nom NXDOMAIN), RCODE 3 comme décrit dans le RFC 1035 et RFC connexes.

Cette disposition s'applique pour tous les fichiers de zone DNS à tous les niveaux dans l'arborescence DNS pour lequel l'Opérateur de Registre (ou une société affiliée fournissant des Services d'enregistrement) maintient des données, organise la maintenance, ou tire des revenus provenant de cette maintenance.

L'interdiction sur les wildcards suivants a été ajoutée à la norme 6 de la version 3 de l'Accord de registre :

"Pour les noms de domaine qui soit ne sont pas enregistrés par un demandeur ou le demandeur n'a pas fourni des enregistrements valides tels que des enregistrements NS pour inscription dans le fichier de zone DNS, ou leur statut ne leur permet pas d'être publiés dans le DNS, l'utilisation d'enregistrements de ressources DNS wildcard tels que décrits dans la RFC 4592 ou toute autre méthode ou technologie pour synthétiser les enregistrements des ressources DNS ou en utilisant la redirection dans le DNS par le registre, est interdite. Lorsqu'ils sont interrogés pour de tels noms de domaine, les serveurs de noms faisant autorité doivent répondre par "Erreur de Nom" (également connu sous le nom NXDOMAIN), RCODE 3 comme décrit dans le RFC 1035 et RFC connexes. Cette

disposition s'applique pour tous les fichiers de zone DNS à tous les niveaux dans l'arborescence DNS pour lequel l'Opérateur de Registre (ou une société affiliée fournissant des Services d'enregistrement) maintient des données, organise la maintenance, ou tire des revenus provenant de cette maintenance."

Le rapport SAC041 (pdf) par le SSAC et les rapports d'autres organisations, ont conseillé à l'ICANN d'interdire l'utilisation de la redirection DNS et les réponses DNS synthétisées dans les nouveaux TLD. Les dangers inhérents à la réorientation et la synthèse des réponses sont présents non seulement dans des TLD, mais aussi à des niveaux subalternes du DNS. Cette disposition prévue dans les contrats de Registre est conçue pour résoudre ce problème au niveau du registre.

4. Encourager la suppression des enregistrements orphelins

Dans le cadre de leurs politiques anti-abus publiées, les registres doivent fournir une description de la façon dont ils supprimeront les enregistrements orphelins au moment où une entrée de nom de serveur est supprimée de la zone. Ce qui suit est extrait du Projet de Guide du Demandeur, module 2 des questions au demandeur:

"Prévention des abus et arbitrage : Les demandeurs doivent décrire les politiques et les procédures proposées pour réduire au minimum les enregistrements abusifs et autres activités qui ont un impact négatif sur les utilisateurs d'Internet. ... Les réponses devraient inclure une suppression rapide ou des systèmes de suspension, et des mesures proposées de gestion et de retrait des dossiers orphelins pour les noms retirés de la zone."

Une étude APWG estime qu'environ 3% des domaines utilisés pour le hameçonnage utilisaient des dossiers de "noms de serveurs orphelins", c'est à dire résultant d'un domaine qui a été précédemment supprimé d'un registre. Cela peut créer une entrée de nom de serveur potentielle "refuge sécuritaire" dans ce fichier de zone du TLD's que les malveillants peuvent utiliser pour des enregistrements de domaines délictueux.

5. Obligations pour un WHOIS étoffé

L'opérateur de Registre doit maintenir et fournir l'accès du public aux données d'enregistrement en utilisant un modèle de données Whois étoffé tel que requis par la spécification 4 de la version 3 de l'accord de registre.

"Service WHOIS**.** Jusqu'à ce que l'ICANN spécifie un format et un protocole différent, l'opérateur de registre utilisera un service de publication d'enregistrement de données disponible à la fois par le port 43 et d'un site Web à <whois.nic.(TLD)> conformément à la RFC 3912 fournissant un accès au public libre en requête-base pour au moins les éléments suivants dans le format suivant. L'ICANN se réserve le droit de spécifier d'autres formats et protocoles, y compris le Service d'information des Registres Internet ("IRIS" - RFC 3981 et RFC correspondantes), et sur cette précision, l'opérateur de registre mettra en œuvre cette spécification alternative dès que raisonnablement possible."

L'ICANN a proposé une modification des conditions Whois dans l'accord proposé de nouveau registre, afin d'exiger que tous les registres offrent la production d'un Whois étoffé comme indiqué dans un précédent mémoire explicatif (pdf). En outre, le projet de rapport (pdf) de l'équipe de mise en œuvre des recommandations de formée par l'ICANN IPC indique " l'IRT estime que la fourniture d'informations WHOIS au niveau du registre en vertu du modèle WHOIS épais est essentielle à la protection rentable des

consommateurs et des titulaires de propriété intellectuelle." La mise en œuvre de Thick WHOIS aidera à réduire le comportement malveillant en assurant une meilleure accessibilité et une meilleure stabilité à l'accès aux documents.

6. Centralisation des accès aux fichiers de zone

L'ICANN demandera que les registres permettent l'accès aux données du fichier de zone dans le but de les rendre accessibles via un prestataire centralisé.

Une proposition ou la version proposée de la spécification 4 de l'Accord de registre (sous réserve d'examen technique) prévoit que l'opérateur de registre rende ces données disponibles à la communauté en général :

"2.2.1. Accès général. L'opérateur de registre doit fournir un volume d'accès vers les fichiers de zone pour le Registre du TLD à l'ICANN ou son représentant sur une base continue et d'une manière que l'ICANN peut raisonnablement spécifier de sporadique.

"2.2.2. Dépôt de dossier de zone centrale. Dans le cas où l'ICANN ou son représentant établit un dépositaire central de fichier de zone, l'opérateur de registre fournira toutes les données de fichier de zones à l'ICANN ou à un opérateur tiers du dépositaire désigné par l'ICANN à la demande de l'ICANN. Si un tel dépositaire central de fichier de zone était établi, l'ICANN peut déroger à la seule discrétion de l'ICANN, conformément à la section 2.1 de cette spécification 4. [La présente section 2.2.2 est inclue aux fins de discussion dans la communauté à la suite de discussions communautaires préalables concernant la réduction du comportement malveillant. En vertu de cette disposition, un représentant de l'ICANN pourrait assumer la responsabilité actuellement supportée par les opérateurs de registre de gérer et contrôler l'accès au fichier de zone par les parties responsables à des fins légitimes.]"

Afin de faciliter l'accès aux données du fichier de zone de registre, qui est actuellement géré par les registres individuel,s l'ICANN (ou partie désignée par l'ICANN pour remplir cette fonction) collecterait les données de dossiers de zones des nouveaux registres de gTLD et fournirait aux abonnés un accès électronique aux données. Cela comprendrait également un seul contrat à signer pour les parties souhaitant avoir accès aux fichiers de zone pour les registres réglementés de l'ICANN, que l'ICANN aurait mis en place par les contrats d'accès se basant sur le modèle actuel, et l'administration / gestion du système de transfert.

Cette coordination centrale permettra à la communauté anti-abus d'obtenir efficacement les mises à jour sur les nouveaux domaines quand ils sont créés dans chaque zone.

7. Contact et politiques documentés des niveaux d'abus des Registres et Registraires

L'opérateur de registre doit fournir un point de contact unique pour les abus pour tous les domaines au sein du TLD. Ce contact sera chargé de traiter et de répondre en temps opportun aux plaintes reçues des parties reconnues, telles que d'autres registres, des registraires, des organismes légaux et membres reconnus de la communauté anti-abus. Les registres doivent aussi fournir une description de leurs politiques de lutte contre l'abus.

L'opérateur de registre peut exiger de tous les registraires avec lesquels il contracte pour les services, de fournir un point de contact d'abus. Cette démarche est conforme aux

recommandations du rapport SAC038 du SSAC (pdf). Les registres peuvent également exiger des registraires de publier une politique d'abus documentée cohérente avec la politique de l'abus du registre. Aux deux niveaux, la politique porte sur les procédures par lesquelles :

1. suspension du domaine identifié comme étant impliqué dans l'abus de marque, le hameçonnage, la distribution volontaire de logiciels malveillants ou d'autres activités illégales ou frauduleuses
2. traitement des questions relatives à des revendeurs ou autres distributeurs de services sous leur contrôle
3. suppression des fichiers orphelins associés à un comportement malveillant
4. identification du point de contact d'abus et comment la communication avec ce point de contact devrait se produire

La formulation suivante a été ajoutée à la norme 6 de la version 3 de l'accord de registre pour aborder ce point :

"L'opérateur de registre doit fournir sur son site Internet ses coordonnées précises, dont une adresse email valide et une adresse postale ainsi qu'un contact principal pour le traitement des demandes de renseignements liées à la conduite de malveillance dans les TLD, et informera l'ICANN sans tarder de toute modification de ces coordonnées."

En outre, l'extrait suivant d'un module 2 est inclus dans le Projet du Guide du demandeur, version 3 :

"… Chaque gestionnaire de registre sera tenu d'établir et de publier sur son site internet un unique point de contact chargé du traitement des questions d'abus exigeant une attention immédiate et en fournissant une réponse rapide aux plaintes concernant tous les noms enregistrés dans les TLD par tous les registraires de l'enregistrement, y compris ceux impliquant un revendeur.."

La mise en œuvre de nouveaux registres, éventuellement sur une grande échelle, nécessite de nouveaux contrôles bien définis, et des rôles définis dans le processus d'enregistrement de domaine. Les politiques et les contacts d'abus, tant au niveau du registre et registraire sera une étape fondamentale en permettant aux efforts futurs de combattre le comportement malveillant pour poursuivre et croitre avec l'ajout de nouveaux opérateurs.

8. Disponibilité du processus de Demande accélérée de sécurité de registre

L'ICANN a développé une procédure supplémentaire http://www.icann.org/en/announcements/announcement-01oct09-en.htm, en consultation avec les registres gTLD, les registraires et les experts en sécurité, fondées sur les leçons apprises dans la réponse au ver Conficker, pour fournir un procédé pour les registres d'informer l'ICANN de la situation actuelle ou imminente de sécurité impliquant un TLD générique et de demander une renonciation contractuelle pour les actions que le Registre peut prendre ou a prises pour réduire ou éliminer les problèmes de sécurité.

Une situation de sécurité est définie comme une ou plusieurs des situations suivantes :

a. Une activité malveillante impliquant le DNS à un niveau et une gravité qui

menace la sécurité systématique, la stabilité et la résilience du DNS ;

b. Divulgation non autorisée potentielle ou réelle, l'altération, l'insertion ou la destruction des données du registre, ou l'accès non autorisé ou la divulgation d'informations ou de ressources sur Internet par les systèmes d'exploitation, conformément à toutes les normes applicables ;

c. Des conséquences indésirables potentielles ou réelles pouvant causer ou menacer de causer une panne temporaire ou à long terme d'une ou plusieurs des fonctions essentielles d'un registre TLD générique tel que défini dans le plan de continuité de registre gTLD de l'ICANN (pdf).

L'ERSR est exclusivement pour des incidents qui nécessitent une action immédiate par le registre et une réponse accélérée (dans les 24-48 heures) de l'ICANN. Ce processus ne vise pas à remplacer des demandes qui devraient passer par la politique des Services d'Évaluation du Registre (RSEP) (link).

9. Programme de vérification de hautes zones de sécurité

Afin de faciliter la nécessité globale de la collectivité pour une confiance accrue dans les gTLD sélectionnés, l'ICANN a créé un projet d'encadrement pour un programme de vérification des gTLD. Tel qu'il est actuellement proposé, ce programme de vérification sera entièrement facultatif.

Le choix de ne pas poursuivre la vérification au moment de l'application de nouveaux gTLD ne reflète pas négativement sur le demandeur, ni n'affecte ses notes dans le processus d'évaluation. Le but du programme de vérification est d'établir un ensemble acceptable de normes et de critères qui permettront d'améliorer la confiance dans un TLD générique vérifié, à travers l'application de mesures opérationnelles et des contrôles de sécurité, et de mesurer que les registres et les registraires gTLD performent par rapport aux contrôles. Les registres des TLD génériques qui choisissent de poursuivre la vérification seront en mesure de démontrer la vérification par une méthode d'exposition publique, comme un «sceau» ou d'une marque qui est vérifiable par une liste maîtresse des gTLD's vérifiés. L'ICANN va tenir et publier la liste maîtresse des gTLD vérifiés.

En plus de maintenir la liste maîtresse des gTLD vérifiés, le rôle de l'ICANN dans le programme est d'aider à définir, affiner et gérer la gouvernance du programme, et de travailler avec la communauté pour établir les normes de programme et les critères. L'évaluation réelle d'un TLD générique contre les normes du programme et les critères sera effectuée par des entités indépendantes.

Pour parvenir à une vérification du programme proposé, les opérations d'enregistrement doivent être compatibles avec les principes suivants (voir le Guide, module 2) :

a. Le registre montre que l'opérateur maintient des contrôles efficaces pour fournir l'assurance que la sécurité, la disponibilité, la confidentialité des systèmes et des informations supportant le registre critique IT et les opérations commerciales est entretenu.

b. Le registre entretient des contrôles efficaces pour fournir l'assurance que le traitement des fonctions de base de registre est autorisé, exact, complet et réalisé de façon opportune, conformément aux politiques et aux normes établies. L'identité des entités participantes est établie et authentifiée.

c. Le registre entretient des contrôles efficaces pour fournir l'assurance que le traitement des fonctions de base registraire par ses bureaux d'enregistrement est autorisé, exact, complet et réalisé de façon opportune, conformément aux politiques et aux normes établies. L'identité des entités participantes est établie et authentifiée.

Les processus nécessaires à la réalisation de la vérification comprennent une vérification de ces deux opérations d'enregistrement et le soutient des opérations registraires.

Dans le cas où un demandeur souhaite faire une demande pour l'option de vérification, il le fait par un processus en deux phases.

Phase I

Avant la délégation des nouveaux gTLD, le demandeur participe à une évaluation, qui comprendra les éléments suivants:

- Informations générales
- Gestion des domaines / procédures d'arrêt
- Point de contact d'abus et de réponse
- Procédures d'entiercement des documents

Après le nouveau gTLD a été délégué et commencera ses opérations, une période déterminée sera accordé au demandeur afin de mettre en œuvre tous les processus et les contrôles pré-approuvés.

Phase II

La phase suivante teste les processus, les contrôles et des procédures documentés dans la phase I afin de vérifier qu'elles fonctionnent comme prévu. Si des lacunes sont identifiées, elles seront communiquées à l'ICANN par l'organisme d'évaluation indépendant. L'opérateur de registre aura une période définie pour résoudre le problème avant que la demande de vérification du demandeur soit refusée. L'opérateur de registre peut faire une nouvelle demande de vérification à une date ultérieure.

Dans le cas où une nouvelle demande de registre gTLD réussisse l'évaluation et que le TLD est délégué, l'opérateur de registre peut choisir à ce moment de demander la vérification et ensuite passer les tests ci-dessus en une seule phase. Autrement dit, un demandeur peut choisir de prendre les mesures pour obtenir une vérification une fois qu'il a terminé le processus d'évaluation et exploiter ses nouveaux gTLD, plutôt que de le faire simultanément avec le processus d'évaluation.

Les contrôles nécessaires pour appuyer la vérification sont évalués par vérification sur une base périodique afin de conserver le statut gTLD vérifié.

L'ICANN estime que ce programme de vérification permet d'atteindre un degré supérieur de confiance dans les TLD génériques certifiés, au dépends des exigences supplémentaires pour déterminer la précision des contrôles pour le registre, le registraire et le demandeur déclarant ainsi que les opérations d'enregistrement et de registraire. L'équilibre entre la confiance et coûts / bénéfices constitue la décision commerciale clé qu'un registre gTLD utilisera comme base pour déterminer si la vérification est un processus commercial approprié à poursuivre.

Le programme de vérification s'applique à une série d'activités proposée nécessaires pour soutenir une chaîne renforcée de confiance pour les opérations d'enregistrement. L'objectif du projet d'encadrement est sur les contrôles nécessaires pour réduire les risques de comportement malveillant dans les registres gTLD qui choisissent de poursuivre un sceau de vérification de l'ICANN. La portée est limitée aux contrôles et aux activités au niveau des opérations du registre et du registraire, et ne s'étend pas aux opérations des demandeurs. Le programme de vérification a pour but de fournir une raisonnable, mais non absolue, assurance que les données vérifiées gTLD ont des contrôles d'exploitation efficaces répondant aux critères de vérification. L'établissement des critères de vérification et des examens / révisions périodiques indépendantes de leur efficacité, par l'intermédiaire du Programme de Vérification devra donc fournir un niveau accru de confiance.