Consultation publique

Détecter les données d'enregistrement contraires à la Charte de nommage dès la création du nom de domaine

Synthèse des contributions

Janvier 2023

www.afnic.fr | contact@afnic.fr

Twitter : @AFNIC | Facebook : afnic.fr

SOMMAIRE

1. Introduction

La consultation publique sur la détection des données d'enregistrement s'est tenue du 27 juin au 25 septembre 2022, en ligne, sur notre site web (**www.afnic.fr**).

Nous avons reçu dix contributions en réponse à cette consultation publique.

Ce document présente la synthèse de ces contributions.

2. Rappel du projet

Le projet objet de la consultation publique a pour objectif d'identifier **dès la création d'un nom de domaine, et avant sa publication dans le DNS**, les données d'enregistrement des titulaires qui ne respectent pas les critères d'éligibilité de la Charte de nommage du .fr.

Dans un premier temps, nous avons décidé de retenir le critère objectif de **l'éligibilité** d'un titulaire, critère principal d'accessibilité au .fr.

Ce nouveau mécanisme permet de sonder toutes les créations de noms de domaine en .fr et d'identifier **automatiquement** celles pour lesquelles les titulaires ont renseigné un « **code**

Pays » correspondant **à un pays situé en dehors des territoires de l'UE et des pays membres de l'AELE**.

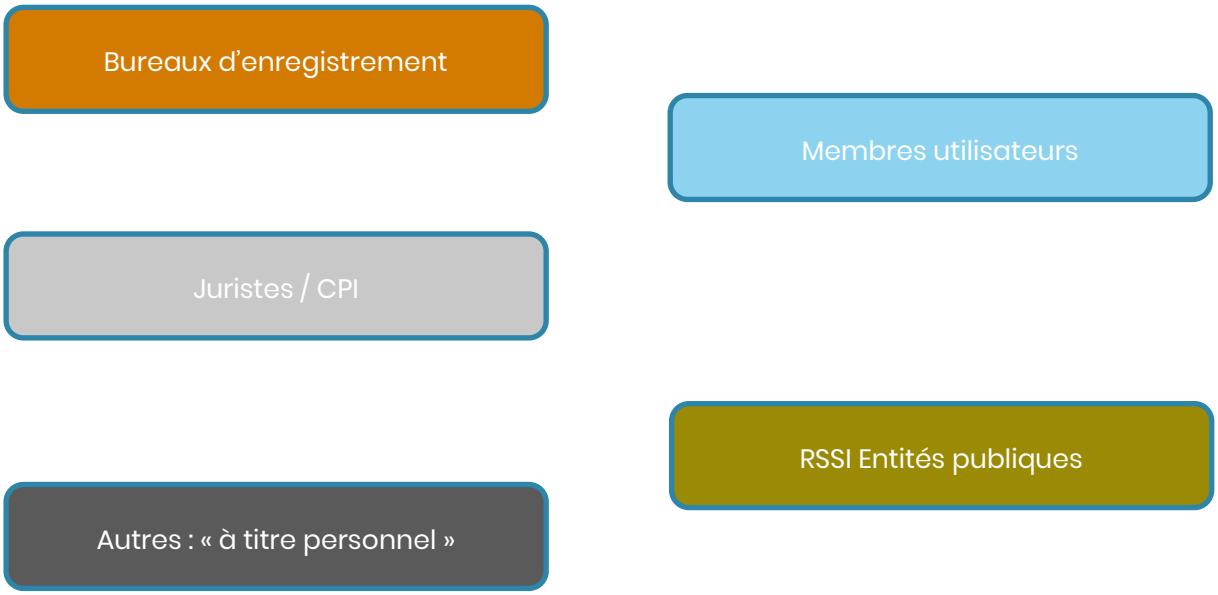
Dès lors que nous détectons un nom de domaine dont les données du titulaire correspondent à cette catégorie, celui-ci est enregistré mais n'est pas publié dans le DNS.

Cela signifie que le nom de domaine est bien enregistré au nom de son titulaire mais que sa **publication dans le DNS est suspendue**. Sous cet état, les services associés au nom de domaine (comme par exemple le site web, l'adresse électronique etc.) ne sont pas de facto ouverts.

Ce projet s'inscrit dans notre dispositif général de lutte contre les abus et plus particulièrement dans **notre objectif de maintenir une base de données dont les informations sont les plus exactes possibles** pour assurer la joignabilité et l'éligibilité des titulaires.

L'ensemble des apports et résultats de la consultation menée, tout au long de l'année 2022, auprès du public et des instances associatives de l'Afnic, seront pris en compte dans le déploiement du projet.

3.Catégories de répondants



4. Accueil du projet

Le projet a reçu un très bon accueil et a été largement relayé sur les réseaux sociaux.

Les contributions reçues proviennent d'intervenants particulièrement compétents et concernés par les thèmes proposés.

Nous n'avons pas relevé d'opposition à ce projet. De nombreuses idées complémentaires ont été proposées.

De manière générale, les répondants reconnaissent que la vérification basée sur le code pays **permettra d'écarter des enregistrements** qui seraient effectués par erreur au nom

d'un titulaire ne répondant pas aux critères d'éligibilité du .fr ou alors qui seraient reconnus comme frauduleux.

Avis / Contributions
La procédure de détection des informations whois ne respectant pas les critères d'éligibilité est une initiative qui devrait se révéler efficace pour préserver la qualité et la confiance de la base .FR tout en préservant la simplicité et l'efficacité d'enregistrement et de gestion des domaines en .FR.
Il parait tout à fait naturel que l'AFNIC puisse dès à présent bloquer ce type de nom de domaine.
La volonté de l'Afnic de détecter les domaines non conformes à la charte de nommage avant publication dans le DNS est évidemment une mesure que je soutiens, et qui répond de façon extrêmement positive à un certain nombre de doutes du grand public sur les moyens mis en œuvre par l'Afnic pour lutter contre les abus.
Ce projet va dans le bon sens, puisqu'il est aisé de détecter tout code pays incohérent. Cette mesure portera ses fruits mais aura rapidement une limite : celle des codes pays FR alors que l'adresse est parfaitement inconnue de la Base Adresse Nationale (BAN). Il n'est donc pas suffisant, et sans attendre les premiers retours de la mise en place de cette mesure, je plaide pour que d'autres suivent rapidement.

5.Synthèse des contributions

Les participants font le constat de **l'évolution des pratiques** en matière d'atteintes en ligne sur le .fr. Ces pratiques visent désormais les utilisateurs des services publics français avec des cas de phishing, typosquatting, d'usurpation d'identité etc.

La majorité des répondants à la consultation publique nous invitent donc à aller plus loin dans la détection que nous proposons de mettre en place.

Cela se traduit par des propositions d'élargissement de la détection à d'autres types de données :

- La détection des **données des titulaires** ;
- La détection des **atteintes liées à l'utilisation du nom de domaine ;**
- La détection des **noms de domaine au moment de l'enregistrement**.

Les répondants font également référence à la **responsabilité des bureaux d'enregistrement** dans ce processus.

Enfin, ils identifient certains **risques** liés au projet.

5.1 La détection des données des titulaires

Avis / Contributions
Restreindre la liste des codes pays autorisés **au moment du dépôt :** Le non-respect d'une condition d'éligibilité basée sur l'adresse doit empêcher purement et simplement la demande d'enregistrement du nom de domaine auprès du BE, donc un blocage a priori.
Vérifier la **concordance** entre le numéro de téléphone fixe et le code postal.
Réfléchir à une solution permettant de **détecter les données fantaisistes** des titulaires personnes physiques.
Faire appel à un **service de vérification/normalisation d'adresse** qui vous permet de vérifier si l'adresse du titulaire existe : filtrage par adresse, par numéro de téléphone etc.
Constituer **une base de données de saisies constatées frauduleuses ou fantaisistes** pour les détecter plus facilement lors de futurs enregistrements.
L'AFNIC en sa qualité de registre doit pouvoir **analyser l'ensemble des données renseignées** pour les réservataires et pouvoir **identifier des patterns whois suspects** en fonction de sites détectés comme suspects via par exemple l'utilisation du classificateur COMAR (**https://www.afnic.fr/observatoire-ressources/papier-**

expert/application-du-systeme-de-classification-comar-a-35-000-url-de-phishing-distinctes/).
Forcer la procédure de vérification d'éligibilité en présence d'un faisceau d'indice suffisant pour démontrer le **caractère suspect, mais cohérent**, des données indiquées par le réservataire.
Faciliter l'ouverture des procédures de vérification en simplifiant les motifs actuellement requis

5.2 La détection des atteintes liées à l'utilisation du nom de domaine

Avis / Contributions
Mettre en place un système de **détection des campagnes d'hameçonnage** ou de distribution de **logiciels malveillants** en s'interférant aux bases de données dédiées au recensement de ces pratiques criminelles.

5.3 La détection des noms de domaine au moment de l'enregistrement

Avis / Contributions
Mettre en un **système d'alerte lors du dépôt** d'un nom de domaine similaire ou quasi identique à une marque, une dénomination sociale etc.
Empêcher tout enregistrement **sans validation en amont**
Développer **une IA pour la recherche syntaxique**, proposant un risque élevé de tentative de phishing dans le nom de domaine
Proposer un **filtrage par « mot-clé »,** méthode qui nécessite un travail important de correction, puisqu'elle génère un certain nombre de **faux positifs** et une adaptation régulière au regard des usages, puisque de nouveaux « mots-clés » peuvent apparaître.

5.4 La responsabilité des bureaux d'enregistrement

Avis / Contributions
Il parait tout à fait naturel que l'AFNIC puisse dès à présent bloquer ce type de nom de domaine, voire **chercher la responsabilité du BE** à ce titre en fonction du **volume** d'enregistrement non conforme à ses engagements contractuels (accréditation et obligation d'information quant à l'éligibilité).
Problème des **proxy** (prête-noms) autorisés par les bureaux d'enregistrement pour des titulaires hors UE.

5.5 Les risques liés au projet

Avis / Contributions
Si blocage automatique d'un nom de domaine au moment de la réservation, risque de pousser le titulaire à recourir à des **méthodes plus « fines »** pour masquer ses actions,

apparaitre en conformité avec les règles du .fr, et rendre ainsi beaucoup plus **complexe le traitement des cas postérieurs**.

Il faut craindre une **professionnalisation** des attaquants qui ne pourront plus ostensiblement renseigner des informations whois erronées et il conviendrait **d'identifier en amont tout autre effet de bord** qui pourrait découler de la mise en place de procédure contraignante à l'issue de cette première consultation.

6. Conclusion

Les contributions à cette consultation publique confirment notre vision de départ dans le contexte des réflexions menées sur une **meilleure définition des abus sur internet et sur les outils de la lutte contre ces derniers**.

Les réponses nous révèlent que les **attentes sont très fortes** sur cette thématique de la lutte contre les atteintes en ligne.

Avec ce projet, notre objectif est de tester les impacts de **la décorrélation de l'enregistrement d'un nom de domaine de sa publication dans le DNS** en le restreignant, dans un premier temps, aux données des titulaires non éligibles au regard de la Charte du .fr.

Cela nous permet de conserver une marge de manœuvre suffisante pour ensuite **faire évoluer le dispositif**, si cela s'avère nécessaire.