Public consultation

Detecting registration data in contravention of the Naming Policy as soon as the domain name is created

Summary of contributions

January 2023

www.afnic.fr | contact@afnic.fr

Twitter: @AFNIC | Facebook: afnic.fr

CONTENTS

1. Introduction

The public consultation on the detection of registration data was held from 27 June to 25 September 2022, online, on our website (**www.afnic.fr**).

We received ten contributions in response to this public consultation.

This document presents a summary of these contributions.

2. Reminder of the project

The aim of the project submitted to public consultation is to identify holder registration data that does not comply with the eligibility criteria set forth in the Naming Policy **as soon as a domain name is created, and before it is published in the DNS**.

From the outset, we decided to use the objective criterion of holder **eligibility**, this being the main criterion for accessibility to the .fr TLD.

This new mechanism allows us to probe all .fr domain name create operations and to **automatically** identify those for which the holders have given the **country code** of a **country outside the EU and EFTA**.

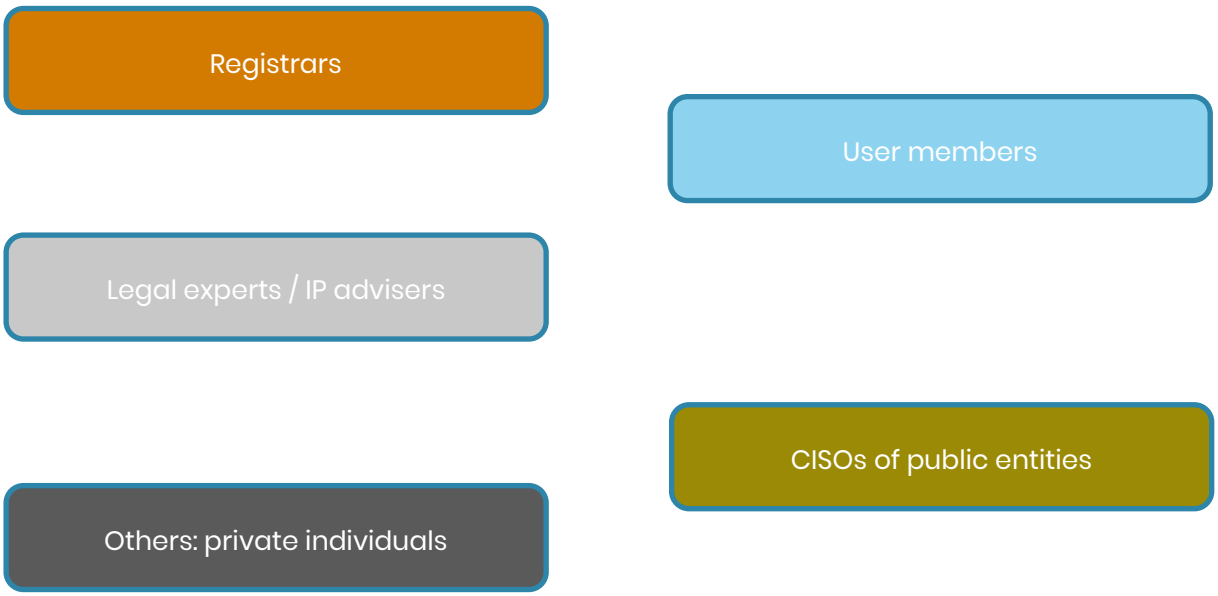
When we detect a domain name for which the holder's particulars correspond to this category, the domain name is registered but not published in the DNS.

This means the domain name is registered in the name of its holder but its **publication in the DNS is suspended**. This being so, the services associated with the domain name, such as the website, email address, etc., are not, de facto, operational.

This project forms part of our overall arrangements for combating online abuse, and contributes more specifically to **our objective of maintaining a database with information that is as correct and precise as possible** to make sure holders are eligible and reachable.

All the contributions and consultation results gathered over the course of the year 2022, from the public and from the internal bodies of Afnic, will be taken into account when we roll out the project.

3.Categories of respondents



4. Reaction to the project

The project has been generally welcomed and broadcast widely on social media.

The contributions received come from particularly competent stakeholders who are and particularly concerned by the proposals.

We have not received any objections to this project. Numerous complementary ideas were put forward.

In general terms, respondents acknowledged that verification based on country codes will **allow the elimination of registrations** made erroneously in the name of holders that do not meet the .fr eligibility criteria or that are flagged up as fraudulent.

Opinions / Contributions
The procedure for detecting Whois information that does not meet the eligibility criteria is an initiative that should prove effective in preserving the quality and reliability of the .FR database while at the same time keeping the registration and management of .FR domain names relatively simple and effective.
It seems only natural for Afnic to now be able to block this type of domain name.
Afnic's determination to detect domain names that do not comply with the Naming Policy before they are published in the DNS is obviously a measure that I support, and which provides an extremely positive response to a number of doubts voiced by the public at large about the resources that Afnic deploys to combat abuse.
This project is a move in the right direction, since it is easy to detect a country code that does not conform. This measure will bear fruit, but will quickly reach a limit: that of FR country codes when the address is completely unknown in the National Address Database (BAN). It is thus insufficient, and I urge those involved not to wait for the initial

feedback on the implementation of this measure, but to move ahead rapidly with other measures.

5.Summary of contributions

The participants noted how **practices had evolved** as regards cyberattacks against the .fr TLD. These practices are now aimed at users of French public services, with cases of phishing, typosquatting, identity theft, etc.

The majority of respondents to the public consultation therefore encourage us to go further in the detection that we propose to put in place.

This translates into proposals to extend the detection to other types of data:

- detection of **holders' data**;
- detection of **attacks linked to the use of the domain name;**
- detection of **domain names at the time of registration**.

Respondents also make reference to **the registrars' responsibility** in this process.

Lastly, they identify certain **risks** associated with the project.

5.1 Detection of holders' data

Opinions / Contributions
Restrict the list of authorised country codes **at the time of filing:** Non-compliance with an eligibility condition based on the address should quite simply put a stop to the requested registration of the domain name with the registrar, in other words block it in advance.
Check that the landline telephone number **matches** the post code.
Give some thought to developing a solution for **detecting fake data** of private individual holders.
Make use of an **address verification/standardisation service** which will enable you to check whether a holder's address exists: filtering by address, by telephone number, etc.
Establish a **database of inputs that have been shown to be fraudulent or fake** so as to be able to detect them more easily for future registrations.
Afnic in its capacity as registry must be able to **analyse all the data provided** for persons seeking to reserve names and be able to **identify suspicious Whois patterns** based on the sites identified as suspect through the use of the COMAR classifier for

example (**https://www.afnic.fr/en/observatory-and-resources/expert-papers/applying-the-comar-classifier-to-35k-unique-phishing-urls/**).

Impose the eligibility checking procedure when there are sufficient indications of the **suspicious nature, even if they are consistent**, of the data input by the person seeking to reserve a name.

Make it easier to start verification procedures by simplifying the reasons currently required

5.2 Detection of attacks linked to the use of the domain name

Opinions / Contributions
Put in place a system to **detect phishing campaigns** or the distribution of **malware** by making use of the databases dedicated to recording these criminal practices.

5.3 Detection of domain names at the time of registration

Opinions / Contributions
Put in place an **alert system on filing** for domain names that are similar or nearly identical to a brand, a corporate name, etc.
Prevent any registration **without upstream validation**
Develop **an AI app for syntactic search**, there being a high risk of phishing in the domain name
Propose **key word filtering,** a method requiring considerable correction work since it generates a number of **false positives,** and a regular adaptation as regards practices since new key words may appear.

5.4 The responsibility of the registrars

Opinions / Contributions
It seems only natural for Afnic to now be able to block this type of domain name and indeed **seek to hold the registrar liable** in this regard depending on the **volume** of registrations not conforming to its contractual commitments (accreditation and obligation to inform as regards eligibility).
Problem of **proxies** ('men of straw') authorised by registrars for holders outside the EU.

5.5 The risks associated with the project

Opinions / Contributions
Automatically blocking a domain name at the time of reservation risks pushing the holder to resort to **more subtle ways** of masking their actions and appearing to conform to the rules of .fr, and this risks making the **treatment of subsequent cases much more complex**.

We have to assume, unfortunately, that attackers will become more **professional,** as they will no longer be able to barefacedly provide erroneous Whois information, and efforts should be made to **identify any other side effects** that might derive from the implementation of the restrictive procedure at the end of this first consultation.

6. Conclusion

The contributions to this public consultation confirm our initial view in the context of the consideration given to **better defining online abuse and to tools for combating it**.

The responses reveal that **expectations are very high** on this subject of combating online attacks.

With this project, our objective is to test the impacts of **the decorrelation of registration of a domain name from its publication in the DNS** by restricting it, initially, to holder data that are not eligible according to the .fr Naming Policy.

This allows us to retain sufficient room for manoeuvre to subsequently **develop the system** if it should prove necessary.