afnic
internet
made in france

La lettre n°5

Édito

Bienvenue dans la cinquième édition de La Lettre Afnic. Cette publication trimestrielle, dédiée à la gouvernance technique de l'internet, a pour ambition de vous tenir informés des développements les plus récents, des enjeux stratégiques et des opportunités qui façonnent l'écosystème de l'internet en général, et de la gestion des noms de domaine en particulier. Nous espérons que sa lecture sera enrichissante.

1

Comprendre DNSSEC, le protocole de sécurité du DNS qui renforce la fiabilité de la résolution de noms de domaine

Le 30 janvier 2024, le domaine internet russe .ru a connu une panne massive d'environ trois heures, mettant hors ligne les sites et moteurs de recherche du pays. Comme c'est souvent le cas dans de telles situations, l'incertitude initiale sur les raisons de cette panne a donné lieu à toutes sortes de spéculations et théories, certaines suggérant des liens avec le contexte de guerre en cours, d'autres pointant du doigt les pratiques de censure du pays. Toutefois, des analyses plus approfondies ont révélé la véritable cause, purement technique et liée à DNSSEC.

Pour comprendre comment ce protocole de sécurité du DNS, censé protéger le réseau, a pu être à l'origine d'une interruption de service d'une telle ampleur, il faut tout d'abord comprendre comment fonctionne la résolution de noms de domaine et comment DNSSEC en garantit l'intégrité.

Comment fonctionne la résolution de noms de domaine ?

Lorsqu'un utilisateur cherche à se rendre sur un site internet – https://www.service-public.fr, par exemple –, il va entrer la requête dans son navigateur web. Débute alors le processus de résolution de noms de domaine, qui va consister à traduire un nom de domaine convivial en une adresse IP que les machines du réseau sauront comprendre.

Lorsque l'utilisateur saisit l'URL dans son navigateur, la requête est envoyée au serveur DNS *(Domain Name System)* local, également appelé résolveur. Celui-ci va envoyer une requête à un serveur DNS racine, qui va lui indiquer quels sont les serveurs faisant autorité (c'est-à-dire compétents) pour l'extension recherchée, dans notre exemple le .fr. Le résolveur envoie ensuite une requête aux serveurs du .fr, qui vont lui indiquer en retour le serveur sur lequel le nom de domaine service-public.fr est hébergé. Le résolveur va enfin demander au serveur qui héberge le nom de domaine service-public.fr l'adresse IP correspondante, avant de renvoyer l'information à l'utilisateur et permettre à son navigateur de se connecter au serveur web hébergeant le site et de l'afficher.

La mise en cache des données de résolution pour gagner en rapidité et en efficacité

Après avoir reçu l'adresse IP du serveur hébergeant le site https://www.service-public.fr, toujours pour l'exemple, le résolveur peut choisir de stocker cette information dans son cache local (soit sa propre mémoire). Chaque entrée dans le cache est associée à un *Time-To-Live* (TTL), représentant la durée de vie maximale de la donnée dans le cache.

Pendant la période de validité du TTL, le résolveur peut utiliser l'adresse IP en cache pour répondre à toute nouvelle requête sur service-public.fr sans réitérer l'ensemble du processus de résolution de noms de domaine. À l'expiration du TTL, il va devoir renouveler l'information en passant à nouveau la requête, rafraîchissant ainsi le cache.

La mise en cache dans le DNS présente de nombreux avantages. En stockant en local les résultats des requêtes DNS les plus fréquentes, elle permet d'accélérer le processus de résolution de noms de domaine et de fournir plus rapidement une réponse aux utilisateurs. Elle allège également la charge qui pèse sur les serveurs DNS puisque moins de requêtes leur sont envoyées, ce qui réduit également le trafic sur le réseau et l'utilisation de la bande passante.

Mais la pratique n'est pas sans risque, car elle expose le système à un possible empoisonnement du cache.

Empoisonnement du cache : qu'est-ce que c'est ?

Dans le contexte du DNS, l'empoisonnement du cache est une cyberattaque visant à modifier ou remplacer les informations stockées dans le cache d'un résolveur, dans le but de compromettre la résolution de noms de domaine. Le résolveur utilisera alors ces données erronées durant toute la période de validité de leur TTL pour répondre aux requêtes correspondantes, redirigeant les utilisateurs vers des adresses IP incorrectes ou frauduleuses.

> **Les premières inquiétudes quant à la sécurité du DNS remontent aux années 1990.**

L'empoisonnement de cache peut ainsi rediriger les utilisateurs vers des sites complètement différents de ceux qu'ils cherchaient initialement. Ces sites peuvent être choisis par les attaquants pour diverses raisons, comme la diffusion de logiciels malveillants ou la désinformation. Les attaques de type hameçonnage sont un autre objectif possible – les utilisateurs, persuadés d'être sur un site web légitime, sont incités à divulguer des données personnelles telles que des identifiants de connexion, des mots de passe ou des informations bancaires.

La prise de conscience des failles de sécurité du DNS

Les premières inquiétudes quant à la sécurité du DNS remontent aux années 1990. À sa création, le DNS n'avait pas anticipé de devoir lutter contre des cyberattaques en général, et contre l'empoisonnement de cache en particulier. Aucun outil ou mécanisme de sécurité n'existait alors pour garantir l'intégrité des données de cache dans le DNS.

Des premiers travaux visant à améliorer la sécurité du DNS ont été menés dès le milieu des années 1990, et ont contribué à sensibiliser la communauté internet aux risques associés à l'absence de sécurité intégrée dans le DNS. En réponse à ces préoccupations, plusieurs initiatives ont été lancées. Parmi elles, l'IETF *(Internet Engineering Task Force)* a créé un groupe de travail dédié, baptisé DNSEXT, dès 1999. Celui-ci était chargé de développer des extensions de sécurité pour le DNS, et il a été à l'origine de DNSSEC. Le processus de développement de DNSSEC a été complexe et a impliqué la contribution de nombreux experts. Plusieurs propositions ont été soumises, discutées et améliorées au fil du temps. En 2005, DNSSEC a été officiellement spécifié dans une série de documents RFC *(Request for Comments)* publiés par l'IETF, notamment les RFC 4033 et 4034.

DNSSEC, le protocole de sécurité du DNS qui garantit la fiabilité de la résolution des noms de domaine

DNSSEC (*Domain Name System Security Extensions*) est une extension de sécurité du système de noms de domaine qui utilise des mécanismes de signature cryptographique et des clés cryptographiques pour garantir l'authenticité et l'intégrité des informations de résolution DNS. DNSSEC repose ainsi sur une paire de clés cryptographiques, à laquelle est associé un identifiant appelé "keytag". Les deux clés ont des rôles complémentaires : la première, privée, signe ; la seconde, publique, permet de vérifier les signatures.

Différentes solutions existent pour créer et gérer ces clés cryptographiques, depuis des logiciels libres (comme OpenDNSSEC ou BIND) jusqu'aux boîtiers propriétaires, en passant par des services en ligne ou des bibliothèques de programmation qui simplifient les développements.

DNSSEC suit la hiérarchie du système DNS, qui est structuré en différents niveaux, chacun géré et supervisé par des autorités spécifiques. DNSSEC ajoute des signatures numériques à chaque niveau. Chaque enregistrement DNS est ainsi signé avec la clé privée du serveur DNS qui l'a émis. Et afin d'éviter qu'un attaquant n'utilise son propre jeu de clés, une autorité parente signe la clé publique de l'autorité enfant, et cela se réplique à travers la hiérarchie.

Le modèle généralement adopté pour DNSSEC s'appuie sur deux types de clés : les clés de signature de zone (ZSK pour *Zone Signing Key*) et les clés de signature de clé (KSK pour *Key Signing Key*). La ZSK est utilisée pour signer les enregistrements DNS individuels, tandis que la KSK signe les clés de zone elles-mêmes. Ces clés sont stockées dans des enregistrements DNSKEY associés à l'enregistrement DNS, et leur signature est également incluse dans d'autres enregistrements DNSKEY pour créer une chaîne de confiance complète, garantissant l'intégrité des données DNS.

Pour renforcer encore la sécurité, DNSSEC prévoit le remplacemnt régulier des clés.

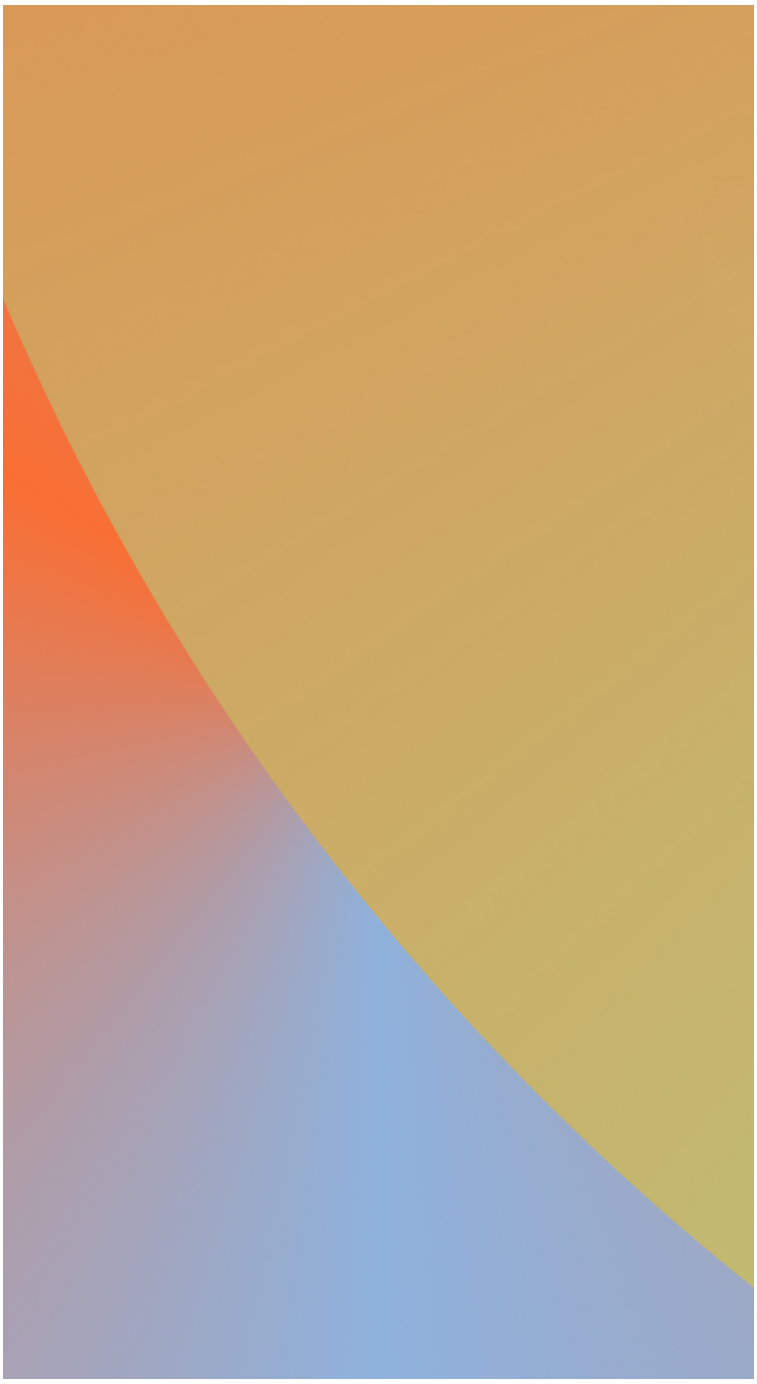
Lorsqu'un utilisateur effectue une requête, le serveur DNS répond avec les données signées. Le client utilise la clé publique du domaine pour vérifier la signature. S'il y a correspondance, il peut être sûr que les données DNS n'ont pas été altérées.

Pour renforcer encore la sécurité, DNSSEC prévoit le remplacement régulier des clés. Lors de ce processus, de nouvelles paires de clés sont générées, publiées et utilisées pour signer les données DNS. Avant de retirer complètement les anciennes clés, une période de chevauchement permet aux anciennes et aux nouvelles clés de coexister. Une fois la période de chevauchement écoulée, lorsque la nouvelle clé a été adoptée par l'ensemble du système, les anciennes clés peuvent être retirées en toute sécurité. Ce processus de remplacement des clés permet de maintenir la sécurité du système DNS en s'assurant que les clés utilisées pour signer les enregistrements sont régulièrement mises à jour et renforcées.

DNSSEC : adoption, déploiement, sensibilisation

Pour fonctionner correctement, DNSSEC doit être déployé d'un bout à l'autre de la chaîne de résolution de noms de domaine – les différents niveaux dont nous parlions plus haut.

- **La racine du DNS constitue le point de départ de toutes les résolutions de noms de domaine.** DNSSEC fonctionnant selon une logique de cascade, il doit être amorcé dès la zone racine. Ce n'est pourtant pas en 2005, à la création de DNSSEC, que la zone racine a été signée, mais en 2010. Le déclencheur : la faille Kaminsky, une vulnérabilité critique dans le DNS mise en lumière en 2008 par le chercheur en sécurité Dan Kaminsky, qui lui a donné son nom. C'est suite à la découverte de cette faille, permettant à des attaquants de manipuler les serveurs DNS et d'introduire des informations malveillantes dans le cache, que DNSSEC a pris de l'ampleur.
- **Les registres forment le deuxième niveau.** Le registre de l'extension .se (pour la Suède) fut le premier à signer sa zone dès 2005 et le premier à ouvrir le service DNSSEC aux titulaires de noms de domaine en 2007. C'est ici encore la faille Kaminsky qui donne un coup d'accélérateur. Dès lors, les adoptions se multiplient parmi les registres, une quinzaine d'entre eux signant leur zone en 2010 – parmi lesquels l'Afnic, le .fr ayant été signé le 14 septembre 2010. Aujourd'hui, si les registres responsables des nTLD (les nouveaux domaines de premier niveau introduits depuis octobre 2013, comme .paris, .bzh, .online, etc.) sont dans l'obligation de signer leur zone avec DNSSEC, il n'en est rien pour les ccTLD (les extensions géographiques). Certains registres de ccTLD n'ont ainsi toujours pas signé leur zone avec DNSSEC.
- **Les bureaux d'enregistrement (BE) jouent également un rôle clé dans la mise en œuvre de DNSSEC** pour sécuriser les domaines de deuxième niveau (SLD, *Second-Level Domain*) – c'est-à-dire la partie du nom de domaine située directement à gauche du domaine de premier niveau (TLD, *Top-Level Domain*) : dans le nom de domaine "servie-public.fr" par exemple, "service-public" est le domaine de deuxième niveau et ".fr" est le domaine de premier niveau.



- **Les serveurs DNS, c'est-à-dire les résolveurs, des fournisseurs d'accès internet (FAI) doivent également être "validants"**, c'est-à-dire capables de prendre en charge et de valider les signatures DNSSEC. Ces résolveurs validants ne constituent pas une obligation pour les FAI, mais ils sont un chaînon essentiel à DNSSEC – au même titre que les serveurs DNS des autres niveaux – pour garantir une infrastructure DNS sécurisée.
- **L'engagement des titulaires de noms de domaine,** enfin, est essentiel au fonctionnement de DNSSEC. Car si le déploiement de cette technologie repose sur les épaules des registres, des BE et des FAI, les titulaires de noms de domaine doivent exprimer la demande de mise en œuvre de DNSSEC pour leurs noms de domaine auprès de leur BE. C'est pourquoi il est important de les sensibiliser à l'utilité de DNSSEC.

Que s'est-il donc passé avec le .ru ?

Comme annoncé dès le 30 janvier 2024 par le Ministère des Communications et des Technologies de l'Information de Russie et confirmé le 7 février 2024 par le *Coordination Center for TLD RU*, le registre qui gère le domaine de premier niveau .ru, dans un message à ses bureaux d'enregistrement, l'incident qui a paralysé l'internet russe était, en toute vraisemblance, dû à un problème lié à DNSSEC.

Il est possible de vérifier l'information en faisant appel à « dig » *(domain information groper)*, une commande système qui permet d'interroger des serveurs DNS pour obtenir des informations détaillées sur des noms de domaine spécifiques, incluant les enregistrements DNS, les adresses IP associées ou encore les signatures DNSSEC.

Ainsi, dans un premier test, on peut constater que les serveurs validants de noms de domaine en .ru indiquaient un statut SERVFAIL au moment de la panne, signifiant qu'il y avait eu une erreur côté serveur lors de la requête. Une analyse plus poussée de la réponse suggère un problème DNSSEC *(« DNSSEC Bogus »)*. Avec la même commande, mais en désactivant la validation DNSSEC cette fois-ci, le résultat montrait une réponse correcte des serveurs *(« NOERROR »)*, incluant les informations demandées sur les noms de domaine en .ru.

Cela permet notamment d'expliquer pourquoi certaines personnes pouvaient toujours accéder aux sites en .ru, tandis que d'autres rencontraient des difficultés, selon qu'elles passaient par des serveurs DNS validants ou non.

Ce premier diagnostic indiquant un problème lié à DNSSEC a pu être confirmé avec DNSViz, un outil en ligne permettant de visualiser le statut d'une zone DNS, dont l'analyse montre clairement des signatures DNSSEC invalides. Zonemaster est un autre outil libre qui aurait pu être utilisé pour effectuer ces tests de validation sur les serveurs DNS.

Tout porte à croire qu'il s'agissait plus précisément d'un problème suite au remplacement des clés DNSSEC, comme une analyse plus approfondie des tests DNSViz le montre. Ces résultats permettent de retracer la chronologie des événements et d'identifier les changements de configuration lors de la panne de l'internet russe :

- Le dernier test correct avant l'incident est enregistré le 30 janvier 2024 à 12h29 UTC. Le numéro de série, qui permet d'identifier la version actuelle de la zone dans son ensemble, était le 4058855. Une opération de remplacement de ZSK est alors en cours, la clé signant les enregistrements étant la 44301, la clé suivante 52263 étant déjà publiée.
- À 15h27 UTC, le premier test montrant des signes de panne est enregistré. Le numéro de série est désormais 4058857. La ZSK 52263 est devenue la clé signante et les signatures sont désormais invalides. Un peu plus tard, une nouvelle zone portant le numéro de série 4058858 est publiée, mais le problème persiste.
- À 17h59 UTC, les réparations débutent. L'ancienne zone avec le numéro de série 4058856 est republiée, l'ancienne clé 44301 reprend du service. Pendant plus d'une heure, plusieurs versions de la zone coexisteront (avec trois numéros de série différents : 4058856, 4058857 et 4058858).
- La réparation s'est achevée à 19h07 UTC, ramenant la situation à celle d'avant la panne.
- Au cours de la journée suivante, la zone a subi une nouvelle modification, avec une nouvelle augmentation de son numéro de série et la signature de la zone avec la clé 52263.

Enfin, on notera que le numéro de série n'a ensuite plus bougé pendant un certain laps de temps (il changeait toutes les deux heures environ auparavant), ce qui fait penser que le problème n'était pas tant dans la clé 52263 que dans le système de signature.

Selon les explications fournies par le *Coordination Center for TLD RU*, le remplacement des clés est une procédure planifiée qui se produit quatre fois par an pour le .ru. Cependant, cette fois-ci, une collision s'est produite avec deux paires de clés ayant le même "keytag", en raison d'une défaillance logicielle. Cela a provoqué un dysfonctionnement dans la configuration du système, touchant plusieurs domaines, notamment ceux en .ru, .tatar et .дети ("дети" signifiant "enfants").

Suite à cette panne, le *Coordination Center for TLD RU* assure désormais travailler à l'amélioration des processus de vérification et de publication des nouvelles clés, ainsi qu'à la modernisation des logiciels utilisés.

Quelles sont les leçons à tirer de la panne du .ru ?

L'incident nous montre tout d'abord que le bon fonctionnement de l'infrastructure de l'internet demande des efforts permanents. Internet est un écosystème complexe, composé de multiples couches d'infrastructures matérielles et logicielles, de protocoles, de serveurs, de réseaux et de services. Toutes nécessitent surveillance et attention pour prévenir les pannes, résoudre les problèmes émergents, mettre à jour les technologies obsolètes, anticiper les nouvelles menaces, etc.

Au sein de cet écosystème, la panne du .ru met particulièrement en lumière l'importance du DNS, car c'est bien un problème de résolution des noms de domaine qui a provoqué un dysfonctionnement généralisé. Le DNS est un service critique dont toutes les applications – ou presque – dépendent. Théoriquement, il serait possible d'accéder à internet sans utiliser le DNS, en mémorisant chacune des adresses IP des sites web que l'on souhaite visiter. Mais dans la pratique, la tentative serait entravée par les méthodes utilisées par les serveurs HTTP telles que le *« virtual hosting »* (qui permet à plusieurs sites d'être hébergés sur une même adresse IP). De plus, la capacité d'HTML à inclure des références vers des ressources externes, soit des images ou encore des scripts hébergés sur des serveurs distincts, et à les charger automatiquement nécessiterait de mémoriser en réalité de multiples adresses IP pour que les sites d'affichent correctement.

La panne du .ru souligne également l'importance des TLD (*Top-Level Domain,* ou domaine de 1er niveau, tel que le .fr) dans la stabilité d'internet. Les noms de domaine sont en effet organisés en arbre. La racine, puis les TLD, puis les domaines de deuxième niveau (SLD, *Second-Level Domain*), etc., forment une structure en arborescence. Cela signifie que tout problème survenant à un niveau va impacter tous les niveaux suivants ; et donc, tout problème au niveau d'un TLD va perturber l'ensemble des domaines qui en dépendent. C'est pourquoi les registres de noms de domaine, qui gèrent les TLD, sont d'une importance cruciale pour le bon fonctionnement d'internet.

Enfin, l'incident du .ru nous rappelle que la cybersécurité requiert des expertises complexes, et un juste équilibre entre la mise en œuvre de mesures de protection rigoureuses et le risque qu'elles puissent engendrer un problème paralysant internet. Toutefois, cela ne doit en aucun cas servir de prétexte pour réduire ou négliger les efforts de sécurité.

02

Plus de 800 000 noms de domaine en .FR créés en 2023 : un record historique

En tant qu'office d'enregistrement du .FR, l'Afnic occupe une position privilégiée pour observer la façon dont la société française fait face aux défis du numérique. Au travers de son Observatoire du .FR, l'association livre bien plus que des statistiques. Ce rapport analyse en effet les tendances et les dynamiques qui animent la présence en ligne des particuliers et entreprises en France, et décrypte comment leurs choix contribuent à façonner la transformation numérique de notre société.

Croissance de +3,4 % du .FR : signe de l'adaptation du marché français au numérique

Les dernières années ont été assez atypiques pour le marché du .FR. La période de confinement due au Covid-19 en 2020 avait incité de nombreuses TPE et PME à accélérer leur présence en ligne, entraînant alors une croissance de +7,0 % du .FR. Ont suivi des années de retour progressif à la normale avec une croissance de +5,8 % en 2021 et +2,9 % en 2022.

En 2023, le .FR affiche une croissance de +3,4 %, avec 4 133 832 noms en stock à la fin de l'année, contre 3 996 245 en 2022. Dans un environnement économique particulièrement incertain, les raisons de cette légère accélération par rapport à 2022 méritent encore d'être confirmées. Elle pourrait toutefois être interprétée comme un indicateur de stabilité et de résilience des entreprises françaises.

Cette croissance de +3,4 % en 2023 est notamment due à une augmentation significative des créations de noms de domaine en .FR (+6,4 %). Un nouveau plus haut historique a d'ailleurs été enregistré avec 801 427 créations : c'est la première fois que le seuil des 800 000 créations annuelles est dépassé.

Plus de 40 % des noms de domaine en France sont en .FR

Le .FR a gagné 0,9 point de part de marché l'année dernière, passant de 39,4 % en 2022 à 40,3 % en 2023. Une tendance à la hausse qui s'observe également sur les cinq dernières années (2019-2023), durant lesquelles la situation du .FR s'est améliorée de manière constante, gagnant au total 3,1 points de part de marché.

On constate également que le .FR croît plus vite que son marché local. Si le .FR s'est développé à la hausse entre 2019 et 2023, le .COM a quant à lui perdu 0,7 point de part de marché en France. Les autres Legacy[1], les autres ccTLD[2] et les nTLD[3] sont également en baisse sur la période, de respectivement 1,9 point, 0,9 point et 0,4 point.

Dynamiques régionales du .FR : entre disparités et rattrapage

La localisation des titulaires de noms de domaine permet d'évaluer le poids de chaque grande région de France. Sans grande surprise, les grands centres urbains et économiques sont aussi ceux qui concentrent le plus grand nombre de noms de domaine en .FR. L'Ile-de-France, en tête avec 28 % du stock, est suivie par l'Auvergne-Rhône-Alpes (12 %), puis la région Provence-Alpes-Côte d'Azur et l'Occitanie (ex aequo avec 8 %). À l'opposé, les régions les plus rurales – Bretagne (4 %), Normandie (3 %), Centre-Val de Loire (2 %), Bourgogne-Franche-Comté (2 %), Ultra-Marins (1 %), Corse (<0,5 %) – sont plus en retrait.

Le classement montre également que le phénomène de rattrapage que l'on peut observer dans certains territoires depuis le Covid s'est poursuivi en 2023. Ainsi, parmi les régions aux plus faibles parts de marché, on retrouve aussi celles aux plus fortes croissances (la Bretagne notamment, +6,3 %). Et à l'inverse, la croissance du stock en Ile de France est parmi les plus faibles (+1,8 %).

Les chiffres variant finalement peu d'une année sur l'autre, il est intéressant d'observer la tendance sur un plus long terme. On peut ainsi constater que, si elle conserve toujours la première place du classement, la région Ile de France a perdu 3,97 points de part de marché depuis 2014. La Nouvelle-Aquitaine (+0,26 points), les Ultramarins (+0,26 points) et l'Auvergne Rhône Alpes (+0,21 points) sont les challengers les plus dynamiques sur la période.

Quelles perspectives pour 2024 ?

L'année 2023 a connu une dynamique exceptionnelle en termes de créations de noms de domaine, ce qui vient confirmer la tendance d'une transformation numérique toujours plus marquée des entreprises françaises.

En 2024, l'Afnic estime la croissance du .FR à environ +2 %, en phase avec les autres ccTLD européens. Ce sera le résultat d'un double défi : maintenir, voire dépasser le nombre de créations de 2023, tout en limitant les suppressions dans un contexte économique incertain.

Pour ce faire, un enjeu majeur pour l'économie numérique française en 2024 sera de sensibiliser les entreprises aux bonnes pratiques numériques. Il s'agira de continuer à accompagner celles qui s'en sont déjà approprié les outils, et de convaincre celles qui sont tentées d'y renoncer de leur intérêt à persévérer. L'objectif étant d'éviter que ne se crée, ou se recrée, une fracture numérique entre entreprises.

1. Les autres Legacy sont ici les extensions génériques, autres que le.com, créées avant 2012 : .aero, .asia, .biz, .net, .org, .info, .mobi, etc.
2. Les autres ccTLD font ici référence aux extensions géographiques correspondant à un territoire ou un pays (par exemple .ca pour le Canada, ou .de pour l'Allemagne), autres que le .fr.
3. Les nTLD sont les nouveaux domaines de premier niveau introduits depuis octobre 2013, par exemple .paris, .bzh, .online, etc.

03

Nouvelles extensions de domaine : le prochain round à l'ICANN est prévu en 2026

Près de 15 ans après le round historique de 2012, qui avait vu près de 2 000 entreprises et organisations postuler pour obtenir leur propre extension de domaine, dont plus de 1 200 ont été introduites dans la racine d'internet, l'ICANN (*Internet Corporation for Assigned Names and Numbers*) s'apprête à réitérer l'expérience et à lancer un autre appel à candidatures en 2026 pour l'obtention de nouvelles extensions de premier niveau (TLD pour *Top-Level Domain*) du système des noms de domaine.

L'organisation américaine à portée internationale, chargée de coordonner et de superviser les aspects techniques et opérationnels des systèmes des noms de domaine et des adresses IP sur internet, travaille actuellement pour préparer ce prochain round de 2026. Quels sont les enseignements tirés du précédent round sur lesquels elle peut capitaliser pour rendre le processus de candidature encore plus efficace et plus inclusif ? Et quelles sont les informations dont nous disposons aujourd'hui sur le déroulement et les modalités de ce prochain round ?

Retour sur le précédent round de 2012

Avant le précédent round d'octroi d'extensions de domaine, il n'existait qu'un nombre assez limité d'extensions internet dites génériques (22 précisément). Les gTLD, tels que le .com, initialement destiné aux entreprises commerciales, le .net, pour les entités impliquées dans les réseaux, ou le .org, pour les organisations à but non lucratif, étaient beaucoup moins nombreux que les extensions de premier niveau national (les ccTLD), telles que le .fr pour la France, le .uk pour le Royaume Uni, etc.

2 000
propositions de nouvelles extensions.

Dans une volonté d'ouverture et de représentation des communautés d'internet, l'ICANN a annoncé en 2009 son intention d'ouvrir un nouveau programme d'octroi d'extensions de domaine, offrant aux entreprises et organisations la possibilité de candidater pour obtenir leur propre extension. Pour les distinguer des *Legacy* gTLD, c'est-à-dire des extensions historiques, déjà existantes, on les appellera new gTLD, pour nouveaux domaines de premier niveau génériques.

Démarré dès 2007, le processus va alors durer plusieurs années. En 2011, l'ICANN publie les règles et les critères de sélection, ainsi que le calendrier prévu. La fenêtre de candidature s'étend ensuite entre mi-janvier et mi-avril 2012 : en 3 mois, l'ICANN recevra près de 2 000 propositions de nouvelles extensions. Les candidatures seront ensuite examinées et évaluées entre 2013 et 2014.

Les nouvelles extensions créées lors de ce round peuvent être classées en trois catégories :

- **Les extensions génériques et spécialisées,** qui représentent un ensemble large et varié d'extensions conçues pour fournir des indications sur la nature du contenu du site web, sur le secteur d'activité ou sur le public cible. Par exemple, .blog pour les blogs, .gay pour la communauté LGBTQIA+, .fashion pour l'industrie de la mode, .bank pour le secteur bancaire, etc.
- **Les extensions de marque,** qui offrent aux entreprises l'opportunité de renforcer leur présence en ligne et de protéger leur identité de marque. Par exemple, .leclerc, .hsbc, .sncf, etc.
- **Les extensions géographiques,** qui font référence à des villes, des régions, des territoires, et visent souvent à promouvoir une identité régionale ou locale en ligne. Par exemple, .bzh, .paris, .alsace, .corsica, .berlin, etc.

Lors de cette ouverture, de nouveaux segments de marché sont créés. Avant cela, les extensions de type .marque n'existaient en effet pas, et aucune ville ne disposait de sa propre extension. Les extensions en caractères non latins, conçues pour répondre aux besoins des utilisateurs dont la langue utilise un alphabet autre que l'alphabet latin (par exemple, l'extension .онлайн (.online) en cyrillique, .ڤكبش (.réseau) en arabe, etc.) y font également leur apparition.

Comment se déroule le processus de candidature ?

S'il reste similaire à celui du précédent round de 2012, le prochain processus de candidature pour obtenir sa propre extension de domaine comportera ces différentes étapes :

Le dépôt de la candidature. Le dossier préparé par les candidats à de nouvelles extensions devra être soumis dans la fenêtre de candidature définie par l'ICANN. En 2012, cette fenêtre avait duré trois mois ; les délais pour 2026 ne sont pas encore précisément connus.

Cette étape impliquera par ailleurs le paiement de frais de candidature. Le tarif pour 2026 reste à déterminer, les discussions actuelles tablant sur un montant d'entrée entre 200 000 $ et 240 000 $ (contre 185 000 $ en 2012).

Les vérifications administratives. Dans un premier temps, l'ICANN vérifiera que le dossier de candidature répond bien à toutes les questions obligatoires, que tous les documents requis ont été fournis, et dans le bon format, et que les frais de candidature ont bien été payés.

L'évaluation des candidatures. Toutes les candidatures complètes feront ensuite l'objet d'une évaluation initiale portant sur deux principaux éléments :

- **Examens des chaînes de caractères.** Cet examen concerne la chaîne de caractères formant l'extension demandée. L'ICANN va vérifier qu'elle ne créera pas de problèmes de stabilité ou de sécurité pour le système de noms de domaine (DNS), en s'assurant que le nouveau gTLD ne causera pas de confusion avec d'autres extensions déjà existantes ou de dysfonctionnement dans le DNS.
- **Examens des candidats.** L'ICANN va ici vérifier que le candidat à un nouveau gTLD possède les compétences techniques, opérationnelles et financières nécessaires pour gérer de manière fiable et sûre le registre associé.

Les candidatures pourront ensuite faire l'objet d'une évaluation plus approfondie permettant de préciser les informations contenues dans la candidature.

La période de consultation publique. Les candidatures seront, en parallèle, soumises à une période de consultation publique, durant laquelle toute personne, organisation, communauté, etc., pourra consulter le dossier de candidature et soumettre un avis sur l'extension proposée.

Une objection formelle pourra alors être déposée pour l'un des quatre motifs suivants :

- **Objection pour confusion de chaînes de caractères.** L'extension présente une trop grande similitude avec un TLD existant ou ayant été déposé dans la même session de candidatures.
- **Droits d'autrui.** L'extension enfreint les droits de la personne ou l'entité qui la conteste.
- **Objection relevant des limitations liées à l'intérêt public.** L'extension est jugée contraire aux principes moraux et à l'ordre public, tels que définis dans les textes de loi applicables au niveau international.
- **Opposition de la communauté.** L'extension fait l'objet d'une forte opposition au sein d'une partie significative de la communauté ciblée implicitement ou explicitement par la chaîne de caractères de l'extension.

En cas de litige ou de conflit durant cette période, l'ICANN va examiner avec attention les arguments présentés et solliciter au besoin des clarifications. Chaque dossier est unique et sera donc traité comme tel, l'ICANN examinant toutes les circonstances avant de prendre une décision. Certaines règles prévalent, notamment :

- **Les droits de marque préexistants.** On parle ici de marques commerciales qui auraient été enregistrées et utilisées avant la candidature. Lorsqu'une candidature est contestée car susceptible de violer des droits de marque préexistants, cela peut entraîner son rejet.
- **La considération de l'intérêt public.** L'ICANN peut également prendre en compte les intérêts publics, tels que la préservation de la culture, de l'identité régionale ou du patrimoine, lorsqu'il y a conflit sur une candidature.
  Ainsi, lors du précédent round, la candidature de la région Aquitaine pour le .aquitaine avait été contestée par une entreprise thaïlandaise de fabrication de fenêtres portant le même nom. L'ICANN avait tranché en faveur de la région française, reconnaissant la primauté des intérêts territoriaux et culturels sur les droits d'une marque privée. L'extension n'avait cependant pas vu le jour à l'époque, en raison du changement de nom et de périmètre de la région entraînée par l'application de la Loi NOTRe.

La signature du contrat et l'attribution. Une fois toutes ces étapes validées, l'ICANN conviera le candidat retenu à signer un contrat en vue de lui attribuer l'extension de domaine.

Le nouveau round à l'horizon 2026 se prépare

En juillet 2023, le Conseil d'administration de l'ICANN a annoncé qu'un dépôt de candidatures pour la création de nouvelles extensions était fixé à mi-2026.

Aujourd'hui, l'ICANN s'est mise en ordre de bataille en mettant en place une nouvelle équipe de direction pour le prochain round. Elle a également officiellement commencé à travailler sur le guide de candidature *(Applicant Guidebook)* – le manuel de référence qui fournit les directives et procédures pour le dépôt d'une candidature. Mais pour l'instant, le calendrier et les modalités restent encore à confirmer.

L'ICANN a en effet lancé quatre programmes en parallèle, qui conditionnent le début du processus de candidature :

- **Un programme de soutien aux candidats.** Ce programme vise à offrir une assistance aux candidats qui pourraient ne pas avoir les ressources nécessaires pour participer au processus de candidature. Cela permet d'encourager la diversité à l'échelle mondiale, favorisant ainsi un accès inclusif et équitable au processus de dépôt des candidatures.
- **L'évaluation des opérateurs techniques de registre en vue de leur accréditation.** Lors de la précédente ouverture, chaque candidature voyait son opérateur technique de registre soumis à un test technique, visant à évaluer ses capacités à fournir des services fiables, sécurisés et conformes aux normes de l'ICANN. Avec ce nouveau processus d'accréditation, l'ICANN entend simplifier et accélérer l'analyse des candidatures et l'intégration des nouveaux TLD, tout en réduisant les coûts. Tout opérateur technique de registre accrédité au préalable serait en effet exempté de test technique.
- **La définition des politiques du programme de candidatures.** Des règles et directives doivent être établies pour préciser le fonctionnement des nouveaux registres de domaine, englobant divers aspects tels que les critères d'éligibilité des candidats ou les procédures de vérification. Elles garantissent notamment la cohérence et la constance dans l'évaluation des candidatures.
- **La gestion du programme dans son ensemble, impliquant son développement et son suivi.** Ce volet constituera la synthèse des précédents points et aboutira à la publication du guide des candidatures puis au dépôt effectif des candidatures.

Une plus forte sensibilisation des marques et des territoires pour 2026

Le précédent round de 2012 avait permis de comprendre comment inciter les territoires et les marques à déposer leur extension, et le rôle de l'ICANN sera aussi pour 2026 de promouvoir leur intérêt et leur utilisation.

Les territoires qui avaient déposé leur candidature en 2012 étaient principalement ceux disposant d'une forte identité régionale et d'une communauté active et engagée. On avait ainsi vu naître en France le .paris, le .bzh, le .alsace ou encore le .corsica. Pour le prochain round, on peut s'attendre à ce que de nouveaux territoires, qu'ils soient locaux ou régionaux, manifestent leur intérêt pour l'obtention de leur propre extension de domaine. Cette tendance pourrait découler d'une volonté de renforcer leur présence en ligne, de promouvoir leur identité, ainsi que d'affirmer leur souveraineté numérique.

Les candidatures pour des extensions en .marque avaient déjà été très nombreuses en 2012, regroupant plus de 700 candidatures. Parmi les secteurs d'activité les plus enthousiastes, le trio de tête comprenait les entreprises des secteurs Banque & Assurance, les constructeurs automobiles et les entreprises technologiques.

Toutefois, beaucoup de marques y étaient allées principalement pour se protéger. De fait, si elles ont obtenu leur extension, très peu l'ont ensuite réellement utilisée. Notons, parmi les cas d'usages réussis, le groupe E.Leclerc, qui a su utiliser son extension .leclerc pour valoriser en ligne son offre de produits (parapharmacie.leclerc, sport.leclerc, etc.) et de services (quiestlemoinscher.leclerc), tout en mettant fortement en avant sa marque. On peut s'attendre, lors de ce nouveau round, à ce que l'intérêt des entreprises pour les extensions en .marque soit tout aussi fort, mais surtout qu'il soit suivi d'usages plus vivants de leurs extensions dédiées.

Un round qui sera, espérons-le, plus fluide et plus rapide

L'ICANN avait été vivement critiquée pour la lenteur des processus lors du précédent round, et de nombreux acteurs plaident aujourd'hui en faveur de cycles de création de nouvelles extensions plus rapides mais aussi plus réguliers.

Parmi les idées évoquées pour gagner en rapidité :

- **L'accréditation des opérateurs techniques de registre,** comme vu plus haut. En certifiant à l'avance les opérateurs techniques de registre, l'ICANN leur accorde sa confiance dans leur capacité à remplir les exigences techniques et opérationnelles nécessaires à la gestion d'une extension de domaine. Cela permettrait de simplifier et donc d'accélérer le processus d'évaluation des candidatures.
- **La création d'un « fast track » pour les candidatures pour des extensions en .marque.** Les extensions en .marque ont un fonctionnement spécifique, généralement dans un environnement fermé avec un seul titulaire *(« single registrant »)*, un seul bureau d'enregistrement et un registre dédié. Cela simplifie considérablement le processus de gestion et de supervision par rapport aux extensions ouvertes. Avec moins de besoins de coordination et de négociation entre les parties prenantes, cela justifierait un traitement à part de ces candidatures plus rapides à examiner. L'ICANN ne semble toutefois pas privilégier cette approche pour le prochain round.
- **Un recours encore plus fort à des prestataires externes pour évaluer les candidatures.** En déléguant une partie toujours plus grande des évaluations à des experts externes spécialisés, l'ICANN va également réduire la charge de travail interne et accélérer le traitement des candidatures. Cela pourrait permettre une évaluation plus efficace et rapide des propositions, tout en garantissant un examen dans les règles de l'art des aspects techniques, juridiques et opérationnels des candidatures.
  On peut noter à cet effet que l'outil utilisé par l'ICANN pour évaluer la conformité technique de la configuration des zones DNS des nouvelles extensions est Zonemaster, service conçu conjointement par l'Afnic et son homologue suédois Internet Stiftelsen.

> **Les candidatures pour des extensions en .marque avaient déjà été très nombreuses en 2012, regroupant plus de 700 candidatures.**

Sur un autre plan, le site web de l'ICANN chargé de recevoir les candidatures avait également rencontré des problèmes techniques majeurs en 2012. Le volume de dépôts était si important que le système n'avait pas réussi à suivre, entraînant de forts retards et même des périodes d'indisponibilité.

Pour faire face à cette situation, l'ICANN avait dû mettre en place une méthode appelée *« Digital Archery »* (tir à l'arc numérique) pour déterminer l'ordre de priorité des candidatures. Ce processus consistait à demander aux candidats de soumettre leur candidature à un moment bien précis, et les candidatures qui s'approchaient le plus de leur horaire cible étaient considérées comme prioritaires : une méthode qui n'était pas restée sans controverse et avait suscité des critiques de la part de nombreux participants. Pour le prochain round, l'ICANN devrait améliorer son infrastructure et ses processus pour éviter que les mêmes problèmes techniques ne se reproduisent.

Enfin, l'ICANN entend consacrer d'importants efforts à la mise en œuvre d'une stratégie de communication afin de sensibiliser les entreprises et organisations aux opportunités offertes par les new gTLD.

Une première phase de cette campagne de sensibilisation a été lancée en mars 2023, mettant l'accent sur l'importance de l'*Universal Acceptance* (acceptance universelle), qui veut que chaque identifiant en ligne, qu'il s'agisse d'un nom de domaine ou d'une adresse email, doit pouvoir être compris et traité de manière équitable et transparente par l'ensemble des infrastructures numériques, au-delà des barrières linguistiques, culturelles et d'écriture. Une série de mini-campagnes a ainsi été lancée, ciblant différents pays – en particulier ceux qui ont eu une exposition limitée au DNS et dont les langues et écritures sont actuellement disponibles dans le DNS[1].

> **L'objectif de l'ICANN est indéniablement de créer un environnement en ligne plus dynamique, inclusif et compétitif.**

La prochaine étape sera de lancer une campagne de sensibilisation pour le programme de soutien aux candidats, avec comme cibles privilégiées les organisations à but non lucratif, les entreprises de l'Économie Sociale et Solidaire et d'autres organisations communautaires de pays et régions en développement.

La deuxième phase de la campagne de communication sera lancée 18 mois avant l'ouverture de la période de soumission des candidatures. Elle visera à fournir plus globalement des informations sur le prochain round et à guider les futurs candidats au travers du processus de candidature.

Dans l'organisation de ce deuxième round, l'objectif de l'ICANN est indéniablement de créer un environnement en ligne plus dynamique, inclusif et compétitif. Et les processus mis en place par l'ICANN pour se préparer au prochain round de candidatures pour les new gTLD démontrent cet engagement à promouvoir un internet ouvert et équitable pour tous.

1. Voir sur ce sujet notre article « Universal acceptance, les défis d'un internet linguistiquement inclusif » dans l'édition n°4 de La Lettre Afnic à destination des décideurs publics.

04 En bref

Le résolveur ouvert européen DNS4EU ne verra pas le jour avant 2025.

DNS4EU est un projet de l'Union européenne qui vise à fournir un service de résolution de nom de domaine (c'est-à-dire un système capable de traduire des noms de domaine en adresses IP) ouvert, européen et sécurisé. DNS4EU permettrait ainsi de renforcer la souveraineté européenne en proposant une alternative aux résolveurs DNS publics actuellement disponibles, bien souvent opérés par de gros acteurs américains. Le consortium retenu par l'Union européenne pour mettre en œuvre DNS4EU, porté par le tchèque Whalebone, a organisé en janvier dernier un webinaire pour faire état de l'avancée du projet. Du chemin reste à parcourir puisqu'y a été annoncé le report à 2025 du déploiement de DNS4EU pour les utilisateurs finaux. Par ailleurs, peu de nouvelles ont été données quant au résolveur public en lui-même. On retiendra avant tout la mise à disposition des FAI (fournisseurs d'accès internet) d'une liste noire DNS4EU de sites web à bloquer par leurs propres résolveurs.

En France, le filtre anti-arnaque poursuit son chemin.

Le filtre anti-arnaque était une promesse d'Emmanuel Macron lors de sa campagne électorale présidentielle de 2022. Son déploiement en version beta pour la Coupe du monde de rugby à l'automne dernier, annoncé en février 2023 par Jean-Noël Barrot, alors ministre délégué chargé de la transition numérique, n'aura finalement pas eu lieu. Le dispositif, censé prévenir les internautes lorsqu'ils se rendent sur un site malveillant, n'en a pas pour autant été abandonné. À l'occasion de son investiture en tant que nouvelle secrétaire d'État chargée du numérique en février dernier, Marina Ferrari a réaffirmé l'importance de son déploiement, qu'elle place dans sa feuille de route de 2024. A cet égard, la commission mixte paritaire sur le projet de loi sur l'espace numérique, son véhicule législatif, a été conclusive le 26 mars dernier. Elle a intégré la définition de l'hameçonnage en ligne et rappelé qu'il constituait bien une forme d'escroquerie au sens de l'article 313-1 du code pénal. Elle a également rétabli une proposition du Sénat donnant la possibilité à l'autorité administrative d'ordonner aux moteurs de recherche ou aux annuaires le déréférencement de sites malveillants faisant l'objet d'une mesure de blocage ou de filtrage.
Mention est aussi ajoutée au site http://cybermalveillance.gouv.fr en cas de message d'avertissement ou sur la page d'information en cas de mesure de blocage pour renforcer l'information et la sensibilisation des utilisateurs.
Le texte a été adopté en séance par le Sénat le 2 avril dernier et par l'Assemblée nationale le 10 avril.

Un groupe de travail « Green » a été créé à l'IRTF.

L'IRTF ou *Internet Research Task Force* est une organisation internationale qui s'intéresse aux défis à long terme liés à l'évolution d'internet. Elle travaille en collaboration avec *l'Internet Engineering Task Force* (IETF) pour améliorer en continu l'architecture et les protocoles d'internet.
La création d'un groupe de travail dédié à l'impact environnemental du web au sein de l'IRTF est le reflet de l'intérêt grandissant de la communauté internet pour ce sujet et de sa participation toujours plus active.
Ce groupe s'intéressera particulièrement aux solutions pour un internet plus durable, avec comme objectif qu'elles soient prises en compte dans les travaux à venir et intégrées aux futurs standards.

Les fournisseurs d'accès internet affichent leur intérêt pour le SMSI+20.

Initié par les Nations Unies, le SMSI ou Sommet Mondial sur la Société de l'Information (également appelé WSIS de l'anglais *World Summit on the Information Society*) est un sommet mondial qui a rassemblé les parties prenantes de l'internet en 2003 à Genève et en 2005 à Tunis. Les enjeux liés à la société de l'information y avaient été discutés, notamment les modalités de la gouvernance de l'internet ou le développement d'un réseau neutre et inclusif dans le monde, créant le Forum sur la gouvernance de l'internet. En préparation du SMSI+20, la revue à 20 ans du sommet mondial, une consultation sous la forme d'un questionnaire a été lancée pour faire le point sur les progrès réalisés, les défis encore à relever et les nouvelles orientations à prendre pour favoriser un développement numérique toujours plus inclusif. Au travers de l'ISPCP (*Internet Service Provider & Connectivity Providers*), l'organisme qui les représente au sein de l'ICANN, les fournisseurs d'accès internet (FAI) ont répondu fin janvier 2024 à ce questionnaire. C'est un signal aussi fort témoignant de l'importance qu'ils accordent aux objectifs du SMSI et aux enjeux de la gouvernance mondiale d'internet.

Les prochains événements auxquels l'Afnic participe :

15 au 19 avril 2024

Commission de la science et de la technique au service du développement, 27ème session

Genève, Suisse

27 au 31 mai 2024

UIT Forum du SMSI 20

Genève, Suisse

4 au 14 juin 2024

Conseil de l'IUT

Genève, Suisse

20 au 26 juillet 2024

IETF 120

Vancouver, Canada

20 au 24 mai 2024

RIPE 88

Varsovie, Pologne

29 et 30 avril 2024

Net Mundial+10

São Paulo, Brésil

10 au 13 juin 2024

ICANN 80 : Forum des politiques

Kigali, Rwanda

30 septembre au 11 octobre 2024

Réunion des groupes de travail du Conseil et des groupes d'experts de l'UIT

Genève, Suisse

15 au 24 octobre 2024

WTSA-24 (Assemblée mondiale de normalisation des télécommunications)

New Delhi, Inde

afnic
internet
made in france

Votre contact

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
7 avenue du 8 mai 1945,
78280 Guyancourt