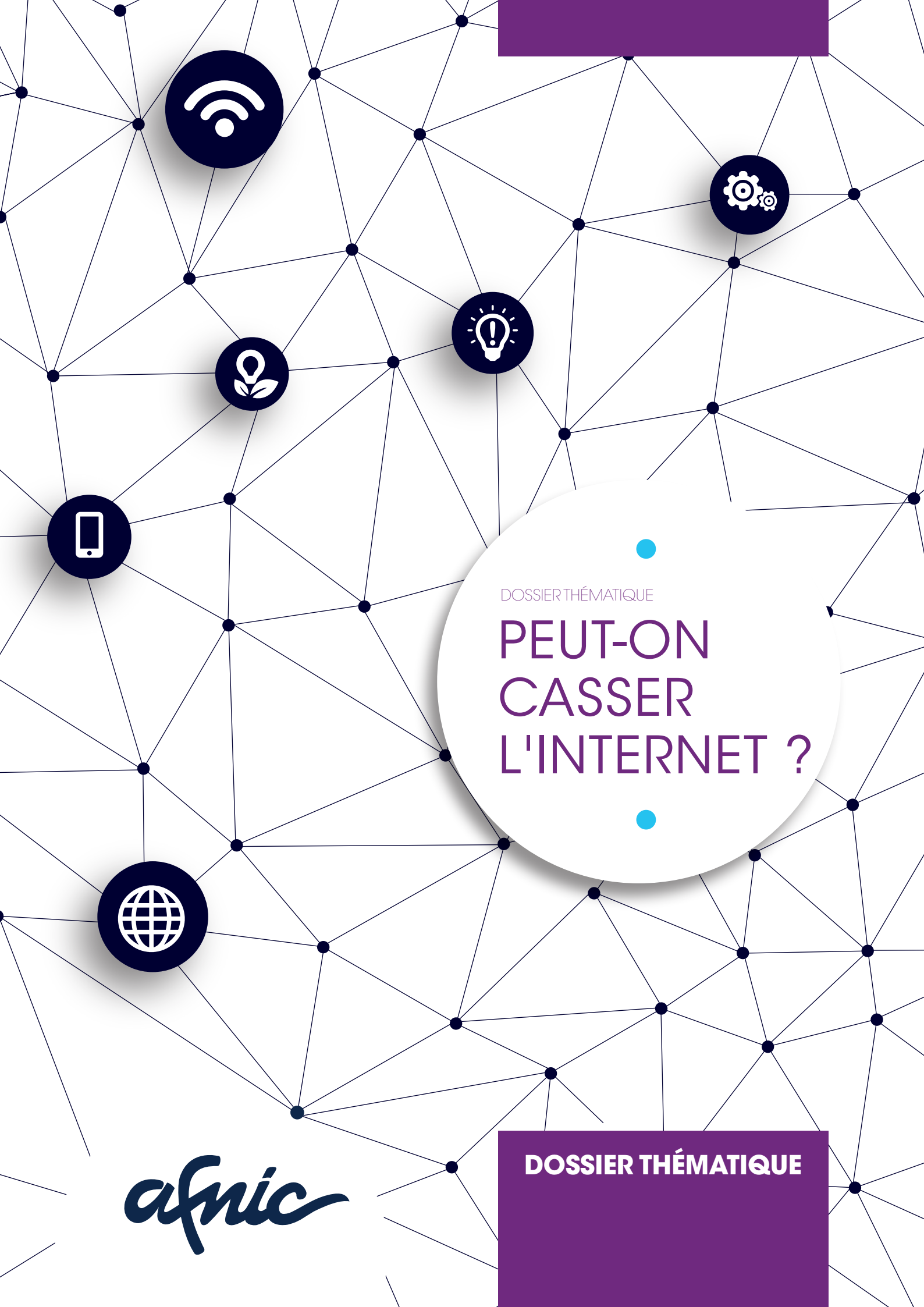


DOSSIER THÉMATIQUE

PEUT-ON CASSER L'INTERNET ?

afnic

DOSSIER THÉMATIQUE

Des incidents spectaculaires, comme la panne résultant de l'attaque contre Dyn le 21 octobre 2016, mènent parfois certains à penser qu'il est possible de casser l'Internet, c'est-à-dire d'interrompre son fonctionnement pendant une période plus ou moins longue. Cette casse pourrait provenir d'une attaque délibérée, ou bien d'une panne accidentelle.

Des articles à sensation ont déjà été publiés sur ce sujet, comme la couverture du Point du 26 janvier 2017 « Le jour où Internet s'arrêtera... La nouvelle cyberguerre mondiale ».

Ce dossier thématique de l'AFNIC va explorer la question de la possibilité d'une telle panne générale. Disons-le tout de suite, la conclusion sera nuancée : on ne peut pas exclure la possibilité d'une telle panne, mais elle ne semble pas un scénario probable. Cela ne veut pas dire que la résistance de l'Internet soit suffisante, ni qu'il faille se reposer.

/// LE VERRE EST-IL À MOITIÉ PLEIN OU À MOITIÉ VIDE ?

Répondre à la question est difficile car la réponse va forcément devoir être nuancée et pleine d'incertitudes. Il est assez facile de prédire le nombre d'accidents de la route qu'il y aura l'année prochaine.

L'expérience (hélas) et la loi statistique des grands nombres ne laissent place qu'à une certaine marge d'erreur. Mais les événements exceptionnels, comme une hypothétique panne totale ou quasi-totale de l'Internet, qui ne se sont jamais produits, sont évidemment bien plus durs à prédire.

Les pessimistes vont en effet dire que les pannes et attaques sont fréquentes, et ont des conséquences sérieuses. Et ils vont citer un rançongiciel bloquant des hôpitaux, un logiciel malveillant empêchant les Rafale de décoller, une attaque par déni de service empêchant l'accès à un site populaire… Et ils vont s'indigner de ce qu'un État, un petit groupe de délinquants, voire un seul lycéen dans son garage, puisse bloquer des services aussi essentiels.

Les optimistes vont remarquer qu'aucune de ces pannes ou attaques n'a arrêté l'Internet, ni même une portion significative de celui-ci. Si gênantes qu'aient été les conséquences pour les utilisateurs de ces services particuliers, l'Internet a continué à fonctionner. Et les conséquences ont été en général de courte durée, c'est-à-dire quelques heures au maximum. On est loin de la « cyberguerre » annoncée.

On peut synthétiser cette apparente opposition de points de vue entre les optimistes et les pessimistes par la fameuse citation de Pierre Col, « ***l'Internet est localement vulnérable et globalement robuste*** ». Il est très facile (trop facile, et il faut y remédier) de provoquer des défaillances limitées dans l'espace et dans le temps, et bien plus difficile de le faire à l'échelle de l'Internet pendant une longue période.

/// MAIS C'EST QUOI, L'INTERNET ?

Une des raisons pour lesquelles les discussions sur la résistance de l'Internet sont difficiles est que beaucoup de gens ne connaissent de l'Internet que ce qu'ils voient sur leur écran. D'où le titre à sensation du New York Times qui annonçait, pendant l'attaque contre Dyn, que « la moitié de l'Internet est cassée ». Pourtant, l'Internet marchait parfaitement pendant cette attaque, même si plusieurs sites très connus étaient affectés.

Il est donc important de rappeler que l'Internet héberge beaucoup de services différents, et ne se limite pas à une demi-douzaine de sites Web. Les entreprises échangent des données, les chercheurs scientifiques copient des fichiers volumineux, le courrier électronique et les services de messagerie instantanée continuent à fonctionner, même si Facebook est en panne.

Les routeurs, le vrai cœur de l'Internet

Quand on parle de l'Internet, on pense surtout aux pages Web des organismes les plus connus, comme Google ou Amazon. Mais la vraie infrastructure de l'Internet, ce sont les centaines de millions de kilomètres de câbles qui relient les ordinateurs entre eux, en passant par les routeurs, ces équipements actifs qui aiguillent les messages vers la bonne direction. Les routeurs du cœur sont nombreux, des centaines de milliers de machines, mais ils sont fabriqués par un petit nombre de constructeurs (comme Huawei, Cisco ou Juniper) et une panne ou une faille de sécurité affectant tout une gamme pourrait avoir des conséquences sérieuses. Là aussi, la diversité est cruciale pour la bonne santé de l'Internet.

Le monde des routeurs est aussi celui du protocole BGP (Border Gateway Protocol), peu sécurisé (et, comme avec le DNS, les solutions de sécurité connues sont peu déployées). Des attaques délibérées, ou des accidents, comme celui commis par Google le 25 août 2017 et qui a coupé une partie de l'Internet notamment au Japon, sont un sujet de préoccupation.

Jusqu'à présent, la coopération entre les opérateurs réseau a toujours permis de mitiger rapidement, puis de résoudre, ces incidents.

Le DNS, un maillon essentiel et souvent oublié de l'infrastructure

Si les câbles, les routeurs, et leur protocole BGP, forment le cœur de l'Internet, le DNS (Domain Name System) est une infrastructure indispensable. Pas de DNS, c'est quasiment pas d'Internet. Et, si vous êtes un peu technicien, ne dites pas « ah, mais on peut taper l'adresse IP pour se connecter ». Avec beaucoup de serveurs Web, cela ne marchera pas ou mal. Il y a parfois plusieurs serveurs sur la même adresse IP, il y a des pages HTML qui chargent du code ou des feuilles de style, via les URL donc des noms de domaine. On voit bien ce caractère crucial du DNS lors des pannes comme celle de Bouygues en avril 2015 ou lors du problème chez Orange en octobre 2016, qui avait classé Wikipédia et Google dans la liste noire par erreur.

Il y a deux sortes de serveurs DNS, très différentes : les **serveurs faisant autorité** sont généralement maintenus par les registres de noms de domaine (comme l'AFNIC, qui maintient les serveurs faisant autorité pour le .fr) ou par des hébergeurs DNS, et les **résolveurs**, qui sont maintenus par les fournisseurs d'accès à l'Internet, les services informatiques locaux ou par des gros opérateurs étrangers.

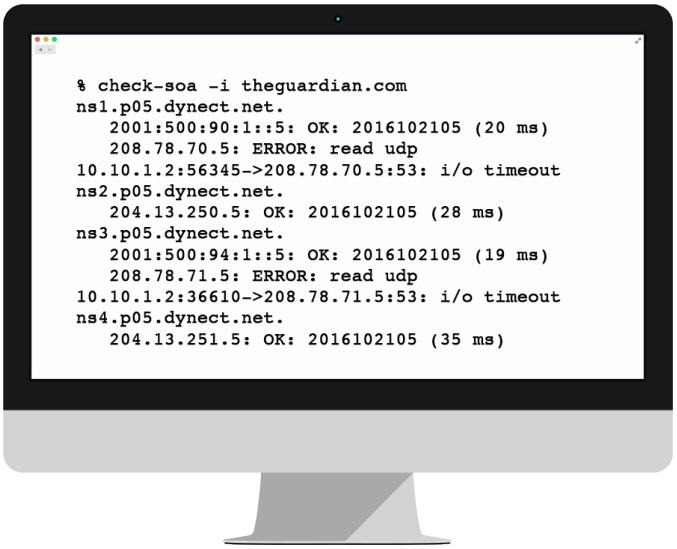
Les deux sont cruciaux, et peuvent faire l'objet d'attaques ou de pannes.

/// ATTAQUE CONTRE DYN EN 2016

Cette attaque par déni de service (attaque qui vise à empêcher un service de fonctionner, pas à en prendre le contrôle) a été une des plus spectaculaires de ces dernières années. Elle a touché, en deux temps, l'hébergeur DNS Dyn le 21 octobre 2016. Elle a frappé en deux phases, d'environ deux heures chacune.

Notez que, contrairement à ce qu'ont affirmé la plupart des médias, la majorité des gros sites Internet connus qui ont été affectés n'étaient *pas clients de Dyn*. Ils étaient clients d'Amazon Web Services, lui-même client de Dyn (les « end-points » AWS dans la région est des États-Unis sont sous le domaine `us-east-1.amazonaws.com` dont tous les serveurs de noms étaient chez Dyn). Il s'agissait donc d'une panne en cascade, fréquente sur le Web d'aujourd'hui, où l'on utilise de nombreux services externes juste pour afficher une page.

On voit ici, avec un outil de mesure en ligne de commande, pour un site de presse qui était client de Dyn, et de Dyn exclusivement, certains des serveurs de noms ne plus répondre. L'attaque consistait à envoyer énormément de trafic vers les serveurs de Dyn, qui ne pouvaient plus répondre à toutes les requêtes légitimes :



L'attaque vue par les sondes RIPE Atlas. SERVFAIL = Server Failure. Undefined (en orange) est une absence de réponse du résolveur.

D'autres domaines, qui étaient chez Dyn et chez un autre fournisseur, n'ont pas eu de problème visible.

/// L'ATTAQUE CONTRE CEDEXIS ET SES CONSÉQUENCES

Le 10 mai 2017, l'hébergeur DNS Cedexis a été victime d'une attaque par déni de service d'une durée d'environ deux heures et demie. Cet hébergeur est notamment utilisé par de nombreux médias, et la presse française était donc peu accessible ce jour. Cette attaque illustre le caractère crucial du DNS, et l'impression de « tout est cassé » que peut donner une attaque réussie sur un service très utilisé par le Web.

Les réseaux sociaux (ici, Mastodon) sont en général le meilleur outil pour apprendre qu'il y a une panne !

Mesuré par l'excellent réseau de sondes RIPE Atlas, voici l'effet sur cent sondes situées en France. La moitié échouent dans la résolution DNS (SERVFAIL = Server Failure) :

```
% atlas-resolve -c FR -r 100 www.sudouest.fr
[195.154.181.181] : 10 occurrences
[ERROR: SERVFAIL] : 50 occurrences
[TIMEOUT(S)] : 33 occurrences
[37.187.142.180] : 5 occurrences
[62.210.93.5] : 2 occurrences
Test #8681136 done at 2017-05-10T13:23:15Z
```

Lisez aussi un interview post-mortem du directeur de Cedexis : (https://www.nextinpact.com/news/104281-retour-avec-cedexis-sur-attaque-ddos-qui-a-rendu-partie-presse-inaccessible.htm).

/// AMÉLIORER LA RÉSILIENCE

En fait, se demander gravement si on peut casser l'Internet totalement ou pas est une question purement théorique. D'une part, il est très difficile de donner une réponse fiable sur ce sujet. D'autre part, il est plus utile de se demander ce qu'on peut faire pour améliorer la résistance de l'Internet.

Par exemple, il y a aujourd'hui bien trop de centralisation chez certains services. Lorsque Facebook est en panne, bien des utilisateurs se plaignent à leur service informatique que « l'Internet est cassé ». Et, en effet, pour eux, cela revient presque au même puisque toutes leurs interactions sont médiées (et enregistrées…) par Facebook.

De manière plus technique, si tous les serveurs DNS sont hébergés chez A. et tous les sites chez C., on voit qu'une panne de A. ou de C. aura des conséquences très étendues. Il est donc crucial que les services Internet, surtout ceux essentiels, soient répartis sur un grand nombre de prestataires différents.

Ces principes de redondance et de diversité doivent guider toute conception de services Internet. La redondance est par exemple d'avoir plusieurs serveurs de noms faisant autorité pour une zone DNS, et qu'ils ne partagent pas un point de défaillance commune (par exemple, ils ne doivent pas être dans la même salle). Autre exemple de redondance, un pays doit être connecté par un grand nombre de liens physiques, très différents. La diversité, elle, recommande de ne pas mettre tous ses œufs dans le même panier. Si tout l'Internet utilise le même logiciel comme serveur DNS, une faille de sécurité dans ce logiciel a des conséquences très étendues.

Notons que l'Observatoire de la résilience de l'Internet en France (https://www.afnic.fr/fr/expertises/labs/projets-realises/l-observatoire-de-la-resilience-de-l-internet-en-france.html) publie un rapport annuel, avec de nombreux indicateurs, comme la variété des opérateurs réseaux pour une zone DNS donnée. (Il contient également plein d'excellents indicateurs BGP.)

Un autre système de mesures, impliquant toute la communauté, est le déploiement des sondes RIPE Atlas (https://atlas.ripe.net), qui permettent de nombreuses mesures techniques depuis les coins les plus reculés de l'Internet.

Comme il est difficile de prévoir les pannes, et encore plus les attaques, les réactions humaines sont cruciales pour faire face aux problèmes. C'est pour cela que coopération, communication et coordination doivent être développées.

Enfin, comme toute œuvre humaine, l'Internet n'est pas parfait et peut défaillir. Il faut intégrer ce risque dans ses évaluations de sécurité et ne pas concevoir des systèmes qui produisent des conséquences dramatiques si l'Internet a un défaut juste à ce moment.

/// EN GUISE DE CONCLUSION…

Si on ne peut pas donner une réponse simple à la question « peut-on casser l'Internet ? », il est possible en revanche de travailler à **améliorer sa résistance** (tenir face aux attaques) et sa **résilience** (repartir après une crise).

En outre, si casser une partie de l'Internet pendant un temps limité reste trop facile, et justifie des efforts en matière de sécurité, casser tout l'Internet pendant une longue durée n'est, heureusement, pas à la portée de n'importe quel attaquant.

RENSEIGNEMENTS UTILES

Contact Afnic

Afnic
Immeuble Le Stephenson
1, rue Stephenson
78180 Montigny-Le-Bretonneux
France
www.afnic.fr

Tél. : +33(0)1 39 30 83 00

@AFNIC

support@afnic.fr

mastodon.social/@afnic

afnic.fr

À propos de l'Afnic :

L'**Afnic** est le registre des noms de domaine .fr (France), .re (Île de la Réunion), .yt (Mayotte), .wf (Wallis et Futuna), .tf (Terres Australes et Antarctiques), .pm (Saint-Pierre et Miquelon).

L'**Afnic** se positionne également comme fournisseurs de solutions techniques et de services de registre. L'**Afnic** - Association Française pour le Nommage Internet en Coopération - est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.