Résilience de l'Internet français
2011 : état des lieux

ANSSI

afnic

Document réalisé par l'ANSSI et l'AFNIC. Recherche et rédaction par : François Contat, Guillaume Valadon, Stéphane Bortzmeyer, Samia M'timet, et Mohsen Souissi.

Vous pouvez adresser vos commentaires et remarques à l'adresse suivante :

rapport.observatoire@ssi.gouv.fr

Table des matières

Introduction **7**

1 Résilience sous l'angle du protocole BGP **9**

1.1 Introduction 9

1.2 Déclaration d'*objets route* auprès du RIPE 14

1.3 Connectivité des AS 20

1.4 Usurpation de préfixes 24

1.5 Conclusion et perspectives 28

2 Résilience sous l'angle de l'infrastructure DNS **31**

2.1 Introduction 31

2.2 Dispersion topologique des serveurs DNS faisant autorité 35

2.3 Taux de résolveurs vulnérables à la faille Kaminsky 39

2.4 Taux de pénétration de DNSSEC 41

2.5 Taux de pénétration d'IPv6 43

2.6 Conclusion et perspectives 47

Conclusion générale **48**

Bibliographie **51**

Acronymes **53**

Résumé

Dans le cadre de l'observatoire de la résilience de l'Internet français, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Association Française pour le Nommage Internet en Coopération (AFNIC) publient un rapport détaillé sur la résilience de l'Internet en France. La résilience de l'Internet, devenue une nécessité, est définie comme sa capacité à fonctionner, et revenir à l'état nominal, lors de la survenue d'incidents. Sur le plan technique, la résilience de l'Internet peut être caractérisée par un ensemble d'indicateurs techniques mesurables.

Ce rapport se fonde ainsi sur des observations concrètes, menées sur plusieurs aspects de l'Internet en France. La résilience d'un système complexe comme l'Internet dépend de nombreux facteurs, parfois difficiles à cerner et à mesurer. Le principe de ce rapport est donc de proposer un certain nombre d'*indicateurs* de la résilience, et de les *mesurer* de façon à appréhender leur pertinence et à mieux comprendre la situation actuelle.

Pour ce premier rapport, nous nous sommes focalisés sur deux protocoles nécessaires au bon fonctionnement de l'Internet : Border Gateway Protocol (BGP) et Domain Name System (DNS). Le premier, BGP, est un protocole de routage, c'est-à-dire un ensemble de règles que doivent suivre les routeurs pour échanger les informations nécessaires au bon acheminement des données entre différents réseaux. Le deuxième, DNS, est le mécanisme par lequel les machines connectées à l'Internet trouvent les adresses IP de leurs interlocuteurs, à partir d'un nom de domaine.

Pour mesurer la résilience de BGP, le rapport a mis en évidence plusieurs indicateurs :

- la déclaration correcte des informations de routage auprès des organismes de gestion des adresses IP, qui permet de vérifier les informations reçues par les routeurs ;
- la connectivité entre opérateurs, qui permet de s'assurer qu'ils ont suffisamment de voisins pour limiter les risques de déconnexion totale ;
- la fréquence du phénomène d'usurpation, par lequel un opérateur annonce ou relaie des informations de routage fausses.

Pour mesurer ces indicateurs, l'ANSSI a analysé la totalité des annonces BGP de quatre acteurs de l'Internet français de grande taille sur une période de onze mois.

Les résultats présentés dans ce rapport sont les suivants :

- la conformité des déclarations de routes et la réalité des annonces BGP varient selon l'opérateur mais aussi selon la période de l'année ;
- cinq opérateurs de transit assurent une grande partie de la connectivité des quatre opérateurs français étudiés ;
- les usurpations de routes sont très fréquentes mais la très grande majorité sont le résultat d'erreurs humaines, notamment dans les relations client/fournisseur, et non de détournements délibérés.

Pour le protocole DNS les indicateurs mesurés sont :

- la « dispersion » des serveurs de noms : selon les pays et les opérateurs ;
- le nombre de serveurs DNS qui n'ont pas été corrigés pour une faille majeure (dite « faille Kaminsky ») ;
- l'état du déploiement de certains protocoles comme IPv6 ou DNS SECurity extensions (DNSSEC).

Les mesures ont revêtu deux formes : les mesures actives auprès des serveurs DNS des domaines de `.fr`, et les mesures passives en observant le trafic DNS entrant sur des serveurs faisant autorité pour `.fr` et administrés par l'AFNIC. Les principales observations concernant le DNS sont :

- pour la majorité des zones sous `.fr`, le nombre des serveurs de noms est insuffisant. Par ailleurs, il pourrait y avoir davantage de serveurs répartis sur plus d'opérateurs ;
- quatre ans après la publication d'une importante vulnérabilité (« faille Kaminsky »), et de sa correction, des serveurs de noms utilisent toujours des implantations logicielles vulnérables ;
- les déploiements de certaines extensions techniques, nécessaires à la pérennité de l'Internet, comme IPv6 et DNSSEC, restent très faibles.

Concernant les protocoles BGP et DNS, le rapport estime, en conclusion, que la situation de l'Internet français est aujourd'hui acceptable, mais que rien ne garantit que cela suffise à l'avenir. Compte tenu du caractère critique de l'Internet dans la société actuelle, il est souhaitable que tous les acteurs s'investissent pour une amélioration permanente de sa résilience.

Introduction

L'Internet est aujourd'hui une infrastructure importante pour les institutions et l'activité économique et sociale dans le monde. Il repose sur un ensemble de composants matériels et logiciels très fortement interdépendants et interconnectés entre eux. Sa structure est un réseau complexe dont le fonctionnement apparaît parfois comme anarchique et difficile à appréhender. Dans les faits, il s'articule autour de différents réseaux gérés indépendamment les uns des autres par des opérateurs de natures diverses (fournisseurs d'accès Internet, diffuseurs de contenu, ou bien encore administrations).

Son caractère massivement distribué constitue à la fois un avantage et un inconvénient pour sa résilience. Sur le plan global, cette distribution limite les risques de panne générale, mais l'interdépendance des acteurs augmente le risque, au moins théorique, de crise systémique. À l'échelle d'un pays comme la France, cette distribution des rôles rend délicate l'identification des risques réels et l'évaluation de leurs impacts.

En parallèle, alors que l'usage de l'Internet se développe très rapidement, les menaces s'accroissent. Les exemples d'entreprises, voire de pays, victimes de pannes ou d'attaques parfois massives, sont désormais nombreux. Face à ces menaces, il faut que l'Internet puisse fournir et maintenir un niveau de service satisfaisant. La résilience de l'Internet est ainsi devenue une nécessité. Au sens strict, la résilience de l'Internet est définie comme sa capacité à fonctionner en mode dégradé pendant toute la durée d'un incident, puis de revenir à un état nominal. Une extension naturelle de la résilience est la robustesse, c'est-à-dire la capacité, en amont, à limiter au maximum les impacts d'un incident sur l'état du système. Sur le plan technique, ces différentes facettes de la résilience de l'Internet peuvent être caractérisées par un ensemble d'indicateurs techniques mesurables.

L'observatoire de la résilience de l'Internet français entend répondre à ces enjeux en identifiant puis en mesurant à intervalles réguliers des indicateurs jugés représentatifs de la résilience. Placé sous l'égide de l'ANSSI, il vise à associer l'ensemble des acteurs de l'Internet français pour définir et rendre compte des informations issues des mesures auprès de ces acteurs et du grand public.

Le principal objectif de cet observatoire est de mesurer le comportement de différents

protocoles critiques pour le bon fonctionnement de l'Internet. L'observatoire cherche ainsi à agréger des informations pour faciliter la détection et la résolution d'éventuels incidents voire de faiblesses structurelles. Un rapport annuel est publié afin de suivre l'évolution de la résilience de manière périodique.

Dans cette première version du rapport, l'observatoire se focalise sur les protocoles BGP et DNS pour donner vie au concept et partager de premiers éléments de réflexion. La liste des indicateurs choisis pour chacun de ces protocoles n'est pas exhaustive et représente un effort conjoint de l'ANSSI et de l'AFNIC. Elle est amenée à évoluer suite aux travaux de l'observatoire et aux discussions avec les acteurs de l'Internet français. Pour chacun des indicateurs, le rapport propose une définition aussi rigoureuse que possible, décrit la méthodologie de mesure associée, et présente les résultats de ces mesures ainsi que leur analyse.

Afin d'appréhender la résilience de l'Internet français sous l'angle des protocoles BGP et DNS, ce rapport utilise les indicateurs suivants.

Pour BGP :

- la déclaration correcte des *objets route* auprès des organismes de gestion des adresses IP, qui permet de vérifier que les informations reçues par les routeurs sont légitimes ;
- la connectivité entre opérateurs, qui permet de s'assurer qu'ils ont suffisamment de voisins pour limiter les risques de déconnexion totale ;
- la fréquence du phénomène d'usurpation, par lequel un opérateur annonce ou relaie des informations de routage fausses.

Pour DNS :

- la « dispersion » des serveurs de noms : selon les pays et les opérateurs ;
- le nombre de serveurs DNS qui n'ont pas été corrigés pour une faille majeure (dite « faille Kaminsky ») ;
- l'état du déploiement de certaines techniques comme le protocole réseau IPv6 ou DNSSEC.

Ce rapport présente, dans le chapitre 1, le fonctionnement du protocole BGP ainsi que les indicateurs de résilience associés ; puis, dans le chapitre 2, le fonctionnement du DNS et les indicateurs associés. Le dernier chapitre tire les conclusions de cette première année de travaux.

Chapitre 1

Résilience sous l'angle du protocole BGP

1.1 Introduction

Chacun des opérateurs de l'Internet gère des blocs, qui sont des plages d'adresses IP (pour *Internet Protocol*) contiguës, qu'il peut diviser en plus petites plages appelées préfixes pour ses propres besoins ou pour ceux de ses clients. Afin de constituer l'infrastructure de l'Internet, les opérateurs se connectent entre eux à l'aide du protocole BGP (pour *Border Gateway Protocol*) défini dans la RFC 4271 [1]. L'objectif de ce protocole est d'échanger des préfixes entre ces réseaux qui sont alors appelés AS (pour *Autonomous System*) et qui sont identifiés par un numéro unique (ASN).

Avant de pouvoir s'interconnecter en BGP, un opérateur doit en premier lieu faire une demande d'attribution d'adresses IP auprès de son organisme de gestion d'IP régional, appelé RIR [1]. Il existe cinq organismes de ce type à travers le monde : l'AfriNIC (Afrique), l'APNIC (Asie et Pacifique), l'ARIN (Amérique du nord), le LACNIC (Amérique latine et Caraïbes), et le RIPE-NCC [2] (Europe, Asie centrale et Moyen-Orient).

Après obtention d'un bloc d'adresses IP, l'opérateur peut, en utilisant le numéro d'AS attribué par son RIR, annoncer ses préfixes IP sur l'Internet en se basant sur un certain nombre de bonnes pratiques. Leur bon usage fait partie de l'étude réalisée dans ce rapport.

Une interconnexion BGP est bilatérale (c'est-à-dire entre deux AS). Chacun des AS échange des préfixes IP et informe son interlocuteur (appelé pair en français et *peer* en anglais) qu'il a la possibilité d'acheminer le trafic à destination de ces préfixes. Les interconnexions se divisent en deux catégories :

1. **le peering ou appairage :** c'est un accord où chaque pair annonce les préfixes qu'il gère. Par exemple, si un fournisseur d'accès à Internet et un diffuseur

1. Pour *Regional Internet Registry* [2].
2. Pour *Réseaux IP Européens*, et *Network Coordination Center*.

de contenu passent un accord de *peering*, tout le trafic entre ces deux interlocuteurs sera alors échangé directement. Les interconnexions de *peering* se réalisent souvent via des points d'échange, dits IXP (*Internet eXchange Point*), qui sont des infrastructures d'interconnexion distribuées sur plusieurs centres d'hébergement de données. Ces interconnexions peuvent aussi être réalisées au travers d'un lien direct entre les infrastructures propres aux deux opérateurs ;

2. **le transit :** il s'agit là d'un accord commercial entre un client (c'est-à-dire, un fournisseur d'accès à Internet ou un fournisseur de contenu) et son opérateur (appelé transitaire) qui lui permet de joindre le reste de l'Internet. Le client annonce ainsi à son opérateur de transit les préfixes qu'il gère. L'opérateur de transit se charge de propager l'annonce de son client et lui annonce en retour le reste des préfixes constituant l'Internet.

Dans une interconnexion BGP, chacun des routeurs annonce pour chaque préfixe un chemin d'AS[3]. Ainsi, comme représenté dans la figure 1.1, si un routeur de l'AS65550 a appris le chemin 65540 64510 64500 pour le préfixe 192.0.2.0/24, cela indique que pour joindre l'adresse IP 192.0.2.1, un paquet au départ d'une des IP de l'AS65550 traversera successivement les réseaux AS65540 et AS64510 avant d'arriver à l'AS64500. Il convient de noter que l'AS gérant le préfixe se situe à droite dans la liste que constitue un chemin d'AS. En pratique, un message BGP de type UPDATE est utilisé pour indiquer le chemin d'AS associé à un préfixe. Ce message BGP est ainsi responsable de l'apprentissage et de l'annonce des routes. Dans la figure 1.1, le routeur de l'AS65550 possède deux routes différents pour joindre le préfixe 192.0.2.0/24. L'une a été apprise via une interconnexion de peering avec l'AS64500 (en bleu), et l'autre via une interconnexion de transit avec l'AS65540 (en violet). Sans autre information, le chemin d'AS le plus court détermine la route utilisée.

Le protocole de routage BGP s'établit à travers une relation de confiance entre les opérateurs. Actuellement, il n'existe pas de mécanisme d'authentification largement déployé permettant de vérifier si une annonce de préfixe est légitime. Dans le cas d'une interconnexion de *peering*, les préfixes d'adresses respectifs sont clairement identifiés par chacun des interlocuteurs, ce qui permet de rejeter tous les autres préfixes.

En revanche, dans le cas d'une interconnexion de transit, les préfixes qu'exportent chacun des deux interlocuteurs ne peuvent être filtrés en raison du caractère dynamique de l'Internet. Il s'agit du point le plus sensible de l'interconnexion des AS. Des erreurs ou une action de malveillance d'un opérateur peuvent provoquer des incidents allant de l'indisponibilité de réseaux à l'interception de trafic.

3. En anglais, AS PATH.

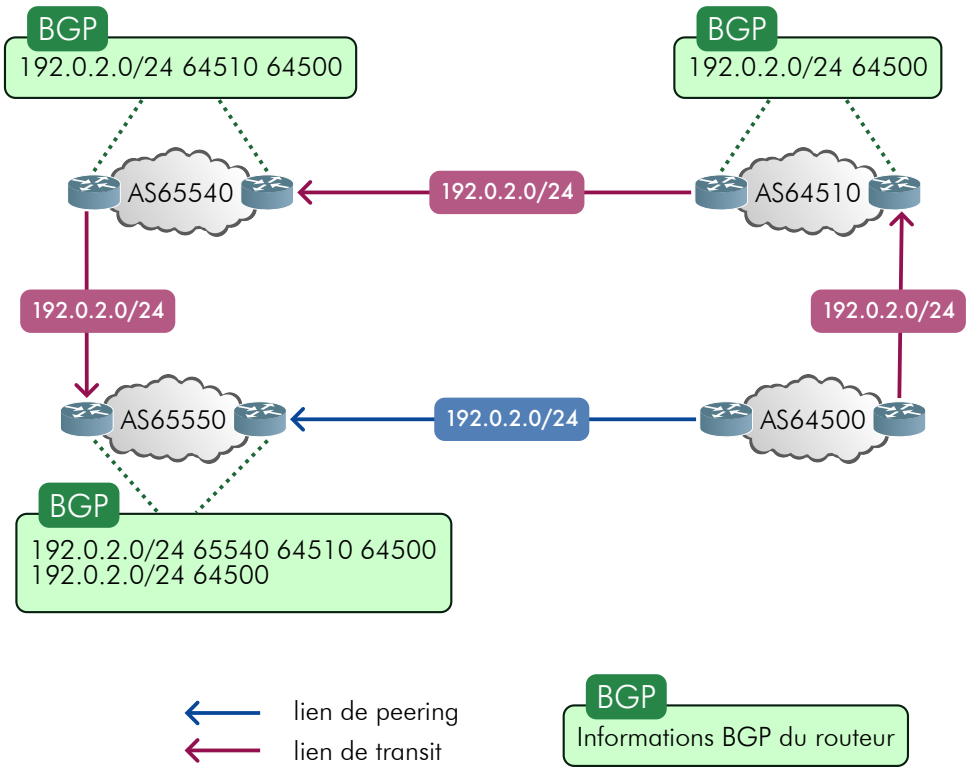

Figure 1.1 - Exemple de chemins d'AS sur des liens de transit et peering

Des travaux effectués à l'IETF [4] ont défini une technologie de signature d'annonces BGP appelée RPKI (*Resource Public Key Infrastructure* [3]). Son objectif est de permettre la signature numérique des annonces afin que la vérification de leur légitimité puisse être automatisée. Le déploiement de RPKI est actuellement coordonné par les RIR. Son utilisation est aujourd'hui marginale mais pourrait s'accélérer ces prochaines années.

1.1.1 Les incidents potentiels liés au protocole BGP

Voici une description des incidents potentiels qui ont été identifiés et dont l'importance est jugée significative :

- **la disparition de préfixes d'adresses :** un préfixe IP peut disparaître de l'Internet si son titulaire en supprime l'annonce auprès de ses pairs BGP. La conséquence directe de cette disparition est l'indisponibilité des réseaux concernés. Ce

4. Pour Internet Engineering Task Force.

genre d'incident est généralement imputable à une erreur humaine ;

- **l'usurpation de préfixe** [5] **:** étant donné qu'il n'y a aucune authentification des annonces de préfixes, il est possible d'annoncer de façon illégitime un préfixe géré par un autre réseau. Les conséquences de ce genre d'incident peuvent être plus ou moins graves selon l'annonce qui est faite. Il est possible que le réseau victime devienne injoignable pour tout ou partie de l'Internet. Une usurpation peut également entraîner une redirection du trafic destiné au réseau victime vers le réseau ayant usurpé les préfixes. Ce genre d'incident provient généralement d'une erreur humaine ;
- **un bogue logiciel sur un équipement :** les routeurs BGP peuvent faire l'objet d'erreurs d'implantation. Ces bogues sont susceptibles d'avoir différents niveaux d'incidence sur le réseau Internet. C'est pour cette raison que les équipementiers sont généralement très réactifs quant à la découverte de bogues et à la mise à disposition de correctifs ;
- **une attaque en déni de service** visant les routeurs BGP : ce type d'attaque n'est pas lié au protocole BGP mais peut, s'il est mené via un réseau à grande capacité de débit, induire une mise hors service de la cible. Ce type d'attaque n'a pas été constaté par la communauté pour l'instant. Néanmoins un certain nombre de solutions simples à mettre en œuvre, comme la RFC 6192 [4], permet de se prémunir de ce type d'attaque.

1.1.2 Objectifs de cette étude

À l'aide d'archives publiques de données BGP concernant l'année 2011, nous cherchons à étudier différents indicateurs de résilience en lien avec les incidents décrits précédemment, pouvant éventuellement avoir un impact sur le protocole BGP, et par conséquent, sur la résilience d'Internet. Aucune attaque en déni de service n'a été rapportée à ce jour.

Dans l'ensemble de ce rapport, nous utilisons des archives publiques de données BGP issues du projet RIS [5], géré par le RIPE. Disposés en différents points du monde, des collecteurs BGP offrent une interconnexion avec des opérateurs et récoltent l'ensemble de leurs tables de routage. Le projet RIS a été mis en place en septembre 1999 et diffuse publiquement l'ensemble des données collectées depuis le lancement de ce projet.

Dans la suite de ce chapitre, nous limiterons notre étude au périmètre de quatre AS français que nous appellerons par la suite AS-fr1, AS-fr2, AS-fr3 et AS-fr4 afin de

5. En anglais, *hijack* BGP.

préserver leur anonymat[6]. Les archives BGP utilisées sont issues du collecteur BGP du RIPE situé à Londres. Il n'y a volontairement pas de correspondance entre les numéros d'AS d'un indicateur à l'autre.

6. Le choix a été fait d'anonymiser les données car la connaissance de l'identité précise des AS ne change rien au constat. Néanmoins, l'analyse ayant été effectuée sur des données publiques, cette anonymisation n'est en réalité que partielle.

1.2 Déclaration d'objets route auprès du RIPE

1.2.1 Description

Lorsqu'un opérateur français souhaite se voir attribuer des blocs d'adresses IP, il en fait la demande directement auprès du RIPE-NCC ou d'un intermédiaire appelé LIR (pour *Local Internet Registry*). En pratique, un LIR est un opérateur capable d'attribuer des adresses IP. Il est important de noter qu'in fine, un opérateur n'est pas propriétaire des blocs d'adresses IP, mais a obtenu une délégation de leur gestion.

L'opérateur peut également décider de découper ce bloc en éléments de plus petites tailles. Ce découpage est par exemple utilisé pour affiner ses politiques de routage, ou pour permettre à ses clients d'annoncer de plus petits préfixes. La relation entre un bloc d'adresses, des préfixes et des adresses IP est illustrée dans la figure 1.2.

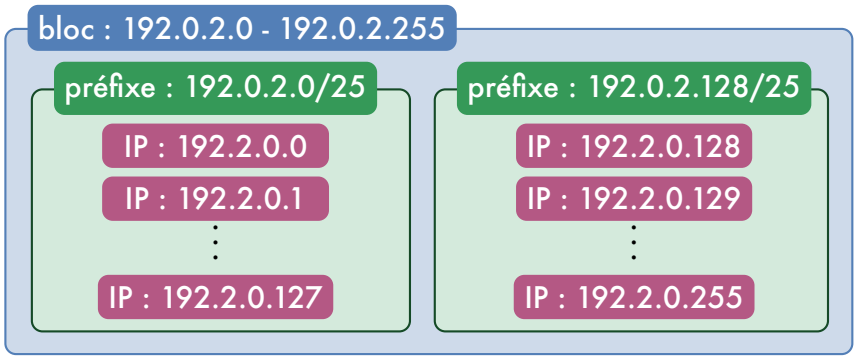

Figure 1.2 - Relations entre blocs, préfixes et adresses IP

Sans plus de précision, il n'est pas possible de savoir si une annonce de préfixes via le protocole BGP est légitime ou non. Pour cette raison, la bonne pratique veut qu'un opérateur déclare les préfixes qu'il annonce en BGP. Ces déclarations sont effectuées par l'intermédiaire d'*objets route* stockés dans un serveur IRR (pour *Internet Routing Registry*). Ce service est généralement opéré par un RIR et rend disponible auprès de la communauté Internet les informations déclaratives des *objets route*. Un *objet route* permet d'identifier clairement le couple AS/préfixe.

La figure 1.3 présente un exemple d'*objet route* dont les principaux attributs sont :

- *route* : le préfixe qui est annoncé en BGP ;
- *origin* : le numéro d'AS qui est à l'origine de l'annonce du préfixe sur l'Internet ;
- *mnt-by* : les personnes en charge de la déclaration et de la maintenance de l'*objet route*.

```
route:          192.0.2.0/24
origin:         AS-64502
mnt-by:         ENTR-FR-1-MNT
```

Figure 1.3 - Exemple d'un objet route

L'étude des *objets route* permet de mettre en évidence les bonnes et les mauvaises pratiques. Ainsi, elle permet également d'anticiper ce qui pourrait se passer si tous les opérateurs filtraient strictement les préfixes sur la base des *objets route*. Dans le cas d'une perte de connectivité avec un transitaire laxiste et la bascule vers un transitaire strict filtrant à l'aide de ces objets, les préfixes non déclarés ne seraient plus propagés. Par conséquent, les services hébergés sur les adresses IP concernées deviendraient injoignables. La déclaration des *objets route* fournit également une méthode simple pour détecter un préfixe annoncé par un opérateur illégitime.

En pratique, une certaine flexibilité existe sur la correspondance entre un *objet route* et des préfixes. Il est ainsi admis qu'un opérateur puisse annoncer des préfixes plus spécifiques que l'objet déclaré. À terme, les *objets route* devraient permettre de systématiser les filtres de préfixes au niveau des routeurs BGP. Par conséquent, les usurpations de préfixes pourront être bloquées au niveau des interconnexions.

1.2.2 Méthodologie de mesure

À l'aide des données disponibles sur le collecteur londonien du RIPE-NCC, et les *objets route* issus de l'IRR, les préfixes annoncés par les quatre AS sont quotidiennement analysés. Pour chaque mois de l'année 2011, nous étudions deux indicateurs distincts pour comparer :

- **les objets route déclarés avec la table de routage** : afin de mettre en évidence la qualité des déclarations d'*objets route* ainsi que les préfixes non annoncés en BGP ;
- **la table de routage avec les objets route déclarés** : afin d'identifier la légitimité des annonces de préfixes sur la base des *objets route* déclarés.

Des statistiques sont calculées mensuellement pour l'ensemble des préfixes IPv4 ayant pour origine les numéros des AS français étudiés dans ce rapport. La période de mesure des données est comprise entre les mois de janvier 2011 et novembre 2011. Les données de l'IRR utilisées sont datées de novembre 2011.

1.2.3 Résultats et analyse

Comparaison des objets route avec la table de routage

La base de travail utilisée est la liste des *objets route* déclarés par chacun des quatre AS comparée à la table de routage globale de l'Internet. Les résultats obtenus sont comptabilisés dans les catégories suivantes :

- **exact** : correspond au nombre de déclarations d'*objets route* dont le préfixe est exactement égal à celui de l'annonce BGP ;
- **approximatif** : correspond au nombre d'*objets route* ayant un ou plusieurs préfixes plus spécifiques dans la table de routage ;
- **multi** : représente le nombre d'*objets route* déclaré par plusieurs AS, dont l'AS observé ;
- **inutilisé** : représente le nombre d'*objets route* n'ayant aucun préfixe annoncé en BGP.

Les données représentées dans le tableau 1.1 sont les valeurs mensuelles médianes sur l'année 2011 ainsi que leurs variations. Afin d'obtenir des pourcentages, les valeurs de chaque catégorie sont divisées par le nombre total d'*objets route* déclarés par l'AS concerné.

Il est important de noter que ces différentes catégories peuvent se recouvrir. En effet, il est possible d'avoir une annonce de préfixe égale à l'*objet route* associé, ainsi qu'une deuxième annonce plus spécifique incluse dans le même *objet route*. Dans ce cas, l'*objet route* sera comptabilisé dans les catégories « exact » et « approximatif ». Par conséquent, la somme des quatre colonnes peut être différente de 100% dans le tableau 1.1.

AS	exact	approximatif	multi	inutilisé
AS-fr1	94.7%	2.6% $^{-/+2.6}$	0%	5.3%
AS-fr2	94.5%$^{-/+5.5}$	0%	0%	5.5%$^{-/+5.5}$
AS-fr3	33.5%$^{-/+0.7}$	19%$^{-/+1.1}$	0%	48.4%$^{-/+3.9}$
AS-fr4	44.6%$^{-/+3.1}$	18.4%$^{-/+6.1}$	17.1%$^{-/+4.3}$	47.7%$^{-/+4.6}$

Table 1.1 - Objets route comparés à la table de routage

Les deux premiers AS analysés montrent des résultats sensiblement proches avec des déclarations auprès du RIPE-NCC ne changeant pas ou peu durant l'année 2011. L'AS-fr1 a 94.7% de ses *objets route* qui sont égaux aux préfixes annoncés, et 5.3%

n'ayant aucun préfixe annoncé. L'AS-fr2 a une tendance similaire à l'AS-fr1 avec une correspondance parfaite entre les *objets route* déclarés et les préfixes annoncés.

Les résultats de l'AS-fr3 et de l'AS-fr4 sont bien plus mitigés. Nous constatons que l'AS-fr3 a des résultats inférieurs aux deux AS précédents : en effet les *objets route* ne sont pas correctement déclarés. De plus, il apparaît que de nombreux *objets route* déclarés ne sont pas annoncés sur l'Internet.

L'AS-fr4 se distingue néanmoins de l'AS-fr3 en deux points. D'un côté, les résultats de la catégorie « approximatif » varient fortement. Cela peut s'expliquer par une forte désagrégation [7] durant la période observée. D'un autre côté, l'AS-fr4 est le seul AS observé avec une valeur « multi » non nulle, certains *objets route* de cet opérateur étant également déclarés par d'autre AS.

Ce premier indicateur permet d'analyser les déclarations d'*objets route* d'un point de vue qualitatif. Il faut toutefois signaler que l'interprétation de ces valeurs dépend fortement de la taille des AS concernés. Il est ainsi plus facile à un AS gérant peu de préfixes d'avoir de meilleurs résultats.

Comparaison de la table de routage avec les objets route

La base de travail utilisée est la liste des préfixes annoncés dans la table de routage globale de l'Internet, comparée aux *objets route* déclarés. Les données ainsi récoltées sont classées dans les catégories suivantes :

- **égal** : cela correspond au nombre de préfixes annoncés en BGP dont la valeur est exactement égale à celle déclarée dans l'*objet route* correspondant ;
- **inclus** : qui correspond au nombre de préfixes annoncés en BGP ayant un *objet route* moins spécifique ;
- **usurpation** : le nombre de préfixes annoncés en BGP ayant un *objet route* déclaré par un autre AS ;
- **non déclaré** : cela correspond au nombre de préfixes annoncés en BGP n'ayant aucun *objet route* déclaré par un AS.

Les données représentées dans le tableau 1.2 sont les valeurs mensuelles médianes sur l'année 2011 ainsi que leurs variations. Les pourcentages sont obtenus en divisant chacune des valeurs par le nombre total de préfixes annoncés. Les données de l'AS-fr4 subissant de fortes variations pendant l'année, le tableau 1.3 fournit l'ensemble des valeurs afin de détailler plus finement la disparité des résultats.

Deux groupes se dégagent très nettement. D'un côté l'AS-fr1 et l'AS-fr2, dont tout

7. C'est-à-dire l'annonce de petits préfixes au lieu d'un grand : par exemple, les quatre préfixes /24 constituant un préfixe /22.

AS	égal	inclus	usurpation	non déclaré
AS-fr1	$95\%^{-/+5}$	$5\%^{-/+5}$	0%	0%
AS-fr2	100%	0%	0%	0%
AS-fr3	$13.5\%^{-/+0.6}$	$74.5\%^{-/+0.9}$	0%	$12\%^{-/+0.3}$
AS-fr4	$13.6\%^{-/+13.4}$	$71.4\%^{-/+21.8}$	$10.1\%^{-/+7.8}$	$13.2\%^{-/+10.2}$

Table 1.2 - Table de routage comparée aux objets route

Mois	égal	inclus	usurpation	non déclaré
01	3.2%	93.3%	2.8%	3.5%
02	25.0%	51.8%	17.9%	23.2%
03	9.9%	80.9%	6.9%	9.2%
04	25.9%	50.9%	17.2%	23.3%
05	26.1%	50.4%	17.4%	23.5%
06	0.2%	82.7%	17.1%	17.2%
07	8.7%	83.7%	5.6%	7.6%
08	27.0%	49.6%	17.4%	23.5%
09	27.0%	49.6%	17.4%	23.5%
10	3.1%	94.0%	2.3%	3.0%
11	22.0%	57.4%	15.6%	20.6%

Table 1.3 - Table de routage comparée aux objets route pour l'AS-fr4

ou partie des préfixes annoncés correspond aux *objets route* déclarés. D'un autre côté, l'AS-fr3 et l'AS-fr4 ont des résultats moins bons sur les catégories calculées : peu de préfixes ont un *objet route* égal. Il est toutefois rassurant de souligner que le pourcentage de préfixes annoncés avec un *objet route* moins spécifique est élevé. Ce chiffre peut s'expliquer de différentes manières :

- un routage plus spécifique pour forcer l'acheminement du trafic ;
- un routage plus spécifique pour faire face à une usurpation ;
- une erreur de configuration.

Sur l'ensemble de la mesure, les résultats de l'AS-fr4 ont une forte disparité d'un mois à l'autre. Il est nécessaire de noter que les valeurs des catégories « égal », « usurpation » et « non déclaré » diminuent fortement lorsque « inclus » augmente. Nous pouvons noter que l'AS-fr4 est le seul AS observé dont les préfixes annoncés sur l'Internet

sont déclarés auprès de l'IRR comme appartenant à d'autres AS. Néanmoins, après investigation, il s'avère que dans la plupart des cas, il s'agit d'entreprises ayant été rachetées, de sous-entités ou de clients de l'AS-fr4.

La comparaison de la table de routage avec les *objets route* met en évidence qu'un certain nombre de préfixes de AS-fr3 et AS-fr4 ne serait pas accepté par un pair BGP filtrant sur la base des *objets route*. Ainsi, les pourcentages de préfixes qui pourraient être bloqués sont donnés par les colonnes « usurpation » et « non déclaré ».

1.3 Connectivité des AS

1.3.1 Description

Dans ce rapport, nous avons arbitrairement choisi d'étudier quatre AS français. L'Internet s'étend cependant en dehors de ces AS au niveau national et encore plus à l'international. À l'aide des archives de routage BGP, il est possible d'identifier les AS interconnectés entre eux : c'est ce que l'on appelle la connectivité. Cette méthode n'est pas exhaustive car la vision est limitée à celle du collecteur BGP choisi, à savoir le collecteur du RIS situé à Londres. Cependant la connectivité fournit une méthode intéressante pour appréhender les interdépendances entre les AS et étudier les interconnexions logiques entre opérateurs.

L'étude de la connectivité des AS permet de représenter la structure de l'Internet français sous forme de graphe. Cette représentation fournit un premier outil efficace pour visualiser les interdépendances entre AS ou comparer les différences entre l'Internet français IPv4 et IPv6.

Il est ainsi possible de mettre en évidence les AS les plus interconnectés avec les quatre AS français étudiés. C'est un premier pas vers l'étude des interdépendances entre AS et l'identification des AS potentiellement critiques pour l'Internet en France.

1.3.2 Méthodologie de mesure

À partir des archives publiques de données BGP du mercredi 30 novembre 2011, des données de l'IRR [8], et de bases publiques de géolocalisation d'adresses IP, nous cherchons à obtenir les indicateurs suivants :

- **une liste non exhaustive des AS français** ou à forte concentration géographique française ;
- **la diversité des connexions**, c'est-à-dire les AS « importants » dont la disparition affecterait de manière significative le fonctionnement de l'Internet français ;
- **le degré de connexion de chaque AS**, c'est-à-dire à combien d'autres AS chacun est connecté.

Nous récupérons tout d'abord la liste de tous les voisins des quatre AS français à l'aide des chemins d'AS contenus dans les archives BGP publiques. Cette liste de voisins nous permet de calculer le degré, c'est-à-dire le nombre de liens, de chaque AS étudié et d'apprécier la diversité des connexions.

8. Ces données comprennent, entre autres, des informations sur les sociétés titulaires des AS, leurs préfixes, et les *objets route* correspondants.

Dans un second temps, à l'aide des données de l'IRR, nous récupérons la liste de tous les préfixes gérés par ces AS voisins. Finalement, nous cherchons à géolocaliser une adresse IP pour chacun des préfixes, afin de déterminer le pays dans lequel pourraient se situer les AS qui les gèrent. Pour ce faire, nous utilisons la base de GeoIP [6]. Cette technique de placement utilisant une seule adresse par préfixe comporte des biais mais fonctionne correctement en pratique.

Il est important de constater que les données utilisées ne permettent pas de mettre en évidence les relations de *peering* entre deux AS, dont la vision est par définition limitée à eux deux. Seules les relations de transit sont mises en évidence. Ainsi la méthodologie appliquée permet uniquement de mettre en évidence les transitaires des quatre AS français ou bien les clients de ces AS.

1.3.3 Résultats et analyse

Parmi tous les voisins des quatre AS, nous avons pu déterminer que 163 d'entre eux sont à forte concentration géographique française. Cette liste n'est pas exhaustive car il en existe peut-être plus, mais la méthode utilisée ne permet pas de les trouver.

Une grande disparité existe parmi ces AS : certains d'entre eux sont de petits clients et d'autres des transitaires. Ainsi, 60% annoncent moins de quatre préfixes. Au total, 1042 préfixes IPv4 sont gérés par ces 163 AS.

Dans un second temps, nous étudions les voisins communs aux quatre AS français afin d'identifier les éventuelles interdépendances. Les cinq numéros d'AS les plus utilisés sont en fait de gros transitaires nationaux et internationaux.

Toutes ces données permettent d'obtenir une vision de l'Internet français centrée sur le collecteur BGP du RIS situé à Londres. La figure 1.4, page 22, a été réalisée à partir de tous les chemins d'AS IPv4 comprenant au moins un des 163 AS français identifiés précédemment. Chaque nœud représente un AS distinct et chaque trait représente une liaison entre deux AS telle que définie par les chemins d'AS. Les quatre AS français étudiés dans ce rapport apparaissent en vert dans la figure, les 159 autres AS français en bleu, et le collecteur BGP du RIS en rouge. Les couleurs des liens correspondent aux nœuds auxquels ils sont connectés, ainsi un lien vert indique une liaison avec l'un des quatre AS français étudiés. Chaque nœud est placé sur un cercle dont le rayon indique la distance par rapport au collecteur du RIS. Les quatre AS étudiés sont ainsi situés à deux sauts de ce dernier.

La figure 1.5, page 23, représente, quant à elle, une vue de l'Internet IPv6 français depuis le collecteur londonien. Elle permet de se rendre compte que l'Internet IPv6 est

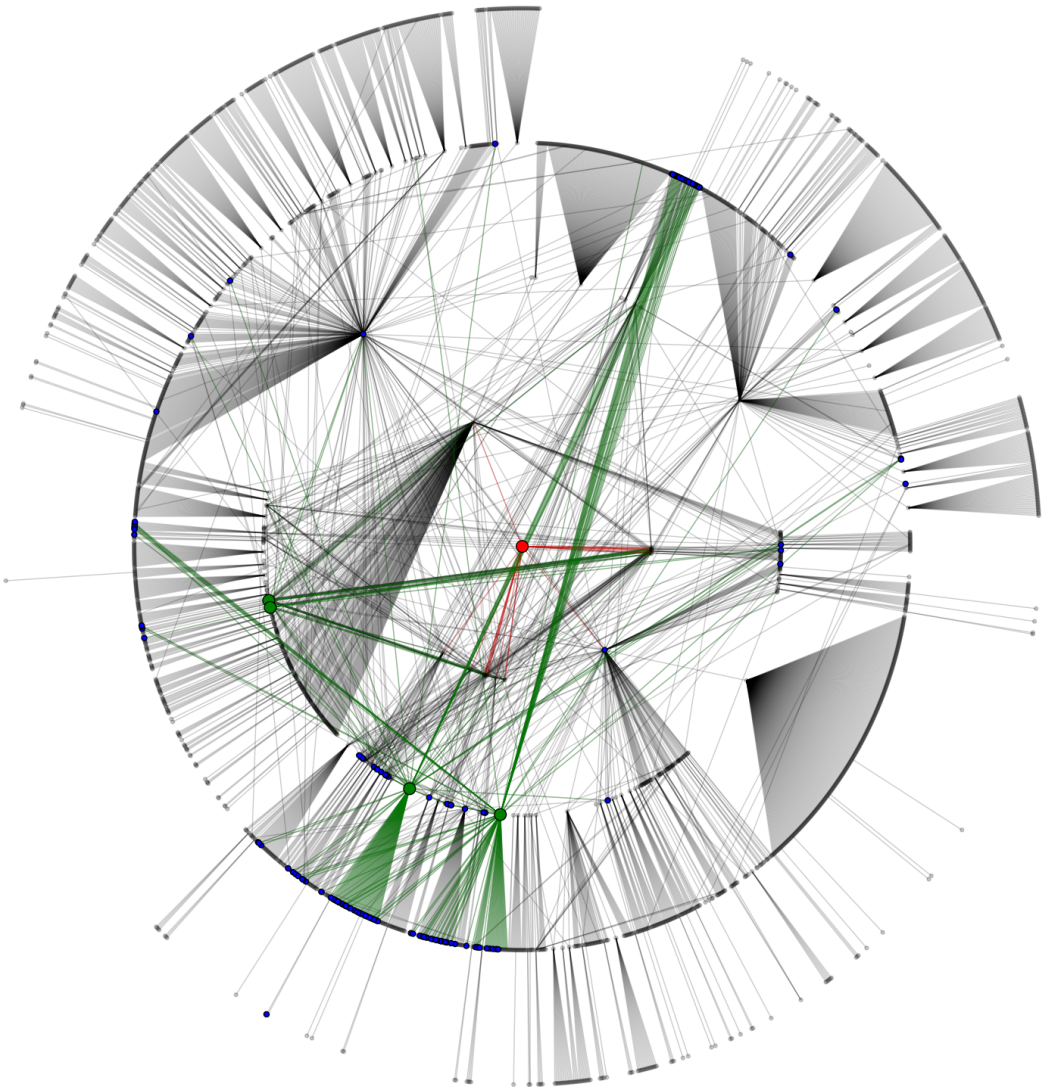

Figure 1.4 - Vue de l'Internet IPv4 français depuis le collecteur BGP du RIPE. En vert, les quatre AS français étudiés. En rouge, le collecteur BGP. En bleu, les autres AS français. En gris clair, des AS étrangers.

actuellement moins dense que l'Internet IPv4, la plupart des 163 AS français n'ayant pas de connectivité IPv6.

Au cours de l'année 2011, le nombre des voisins de chacun des quatre AS étudiés est stable et ne subit pas de changement significatif. Le degré de connexion permet cependant de mettre en évidence deux tendances différentes chez les quatre AS :

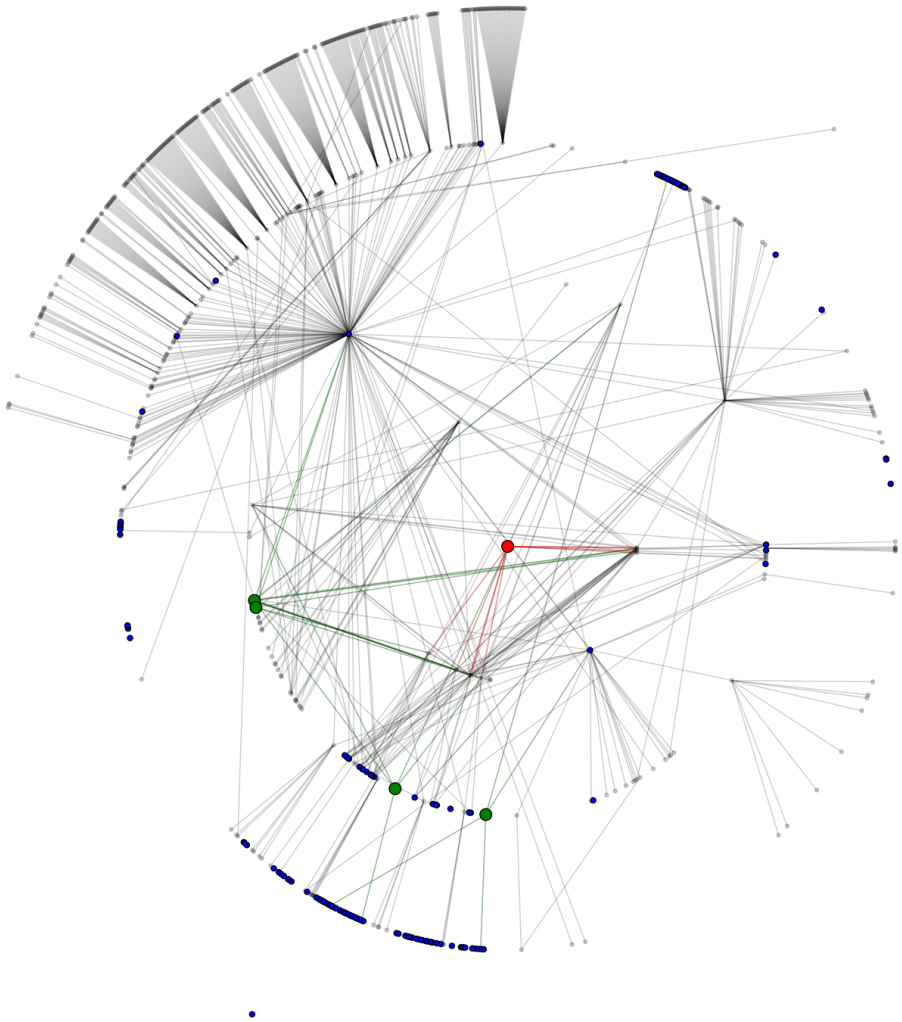

Figure 1.5 - Vue de l'Internet IPv6 français depuis le collecteur BGP du RIPE. En vert, les quatre AS français étudiés. En rouge, le collecteur BGP. En bleu, les autres AS français. En gris clair, des AS étrangers.

ceux qui ont beaucoup de clients (et donc un degré de connexion élevé), et ceux qui en ont peu, ou pas (et donc un degré de connexion faible). Cette constatation est en adéquation avec la réalité, et permet de valider la méthode de calcul des degrés. De plus, la figure 1.4 permet de visualiser très nettement ces deux tendances : les deux AS en vert situés en bas de la figure ont beaucoup plus de liens que les deux autres.

1.4 Usurpation de préfixes

1.4.1 Description

Dans le protocole BGP, il n'existe pas de mécanisme permettant de vérifier si un AS annonce un préfixe de façon légitime. Un AS malveillant peut ainsi annoncer des préfixes dont il n'a pas la délégation.

Les bonnes pratiques voudraient que les opérateurs mettent en place des filtres sur les routeurs BGP leur permettant de limiter, voire de ne pas accepter ce type d'annonces. Ces filtres peuvent être basés sur les *objets route*, sur une déclaration bilatérale des préfixes autorisés, sur le nombre maximum de préfixes acceptés par un pair BGP, ou bien encore sur une combinaison de tous ces éléments.

Dans la suite, nous considérons qu'un préfixe est usurpé si deux AS distincts l'annoncent, ou si un AS annonce un préfixe plus spécifique qu'un préfixe annoncé par un autre AS. Cette définition constitue une première étape dans la détection des usurpations, mais présente quelques limites. Elle ne prend par exemple pas en compte le cas du routage *anycast* [7] dans lequel il est légitime d'annoncer le même préfixe depuis plusieurs AS afin de répartir la charge de trafic.

Dans le cas d'une annonce de préfixe effectuée par deux AS simultanément, il est difficile de prévoir lequel des deux va réellement recevoir les paquets à destination de ce préfixe. De plus, la portée de l'usurpation est difficile à appréhender en raison des diverses interconnexions entre AS, ainsi que de leur distance topologique. Ainsi, si un AS français usurpe un préfixe d'un AS japonais, il est improbable qu'un AS directement connecté avec l'AS japonais puisse être victime de cette usurpation.

À l'inverse de l'indicateur décrit en section 1.2, nous nous intéressons ici à des usurpations de préfixes effectuées depuis tous les AS de l'Internet portant sur des préfixes des quatre AS français étudiés.

Une usurpation de préfixes a pour impact immédiat une redirection partielle ou totale des paquets vers l'AS ayant effectué l'usurpation.

L'analyse des usurpations de trafic permet de mettre en évidence des comportements anormaux dans l'Internet. Dans la majorité des cas, il s'agit d'erreurs humaines de configuration de routeurs BGP. Dans une minorité de cas, il s'agit de véritables usurpations où l'AS usurpateur cherche à récupérer tout ou partie du trafic de la victime, ou à masquer ses propres actions en se faisant passer pour un autre AS.

1.4.2 Méthodologie de mesure

À partir des archives publiques BGP, nous construisons la base des préfixes des quatre AS français étudiés dans ce rapport. Ensuite, nous comparons chaque préfixe annoncé durant l'année 2011 à ceux contenus dans cette base. Dans une première approche, nous considérons qu'il y a une tentative d'usurpation de préfixe, si le préfixe annoncé est plus petit ou égal à ceux contenus dans la base et si l'AS à l'origine de cette annonce est différent de celui contenu dans la base.

Afin de qualifier une tentative d'usurpation de préfixe, l'algorithme mis en œuvre commence par vérifier s'il existe un *objet route* correspondant, auquel cas il s'agit d'une annonce légitime. Si aucun *objet route* n'existe, cette tentative d'usurpation est alors cataloguée dans l'une des deux classes suivantes :

- **usurpation de classe 1 :** l'AS à l'origine de l'usurpation est directement connecté à l'AS usurpé ;
- **usurpation de classe 2 :** l'AS à l'origine de l'usurpation n'est pas directement connecté à l'AS usurpé.

Dans ce rapport, nous ne prenons pas en compte les usurpations portant sur des préfixes appartenant à un AS mais que celui-ci n'aurait pas encore annoncé.

1.4.3 Résultats et analyse

Les quatre AS étudiés dans ce rapport ne sont pas tous concernés par cet indicateur de la même manière. En effet, l'algorithme utilisé n'a détecté aucune usurpation pour l'un d'eux. Trois opérateurs seront donc seulement représentés dans la figure 1.6, page 26.

Les données de l'année 2011 ont été traitées mois par mois de façon indépendante. Ainsi, des traits verticaux apparaissent périodiquement le premier jour de chaque mois et mettent en évidence les traitements successifs des données par notre algorithme ainsi que sa réinitialisation, celui-ci recommençant alors son calcul de zéro. Cette représentation fera l'objet d'une amélioration dans les prochaines éditions de ce rapport. L'axe des ordonnées représente des couples distincts de préfixes usurpés et d'AS usurpateurs.

Chaque mois, le nombre de préfixes usurpés est représenté sur une courbe cumulative, c'est-à-dire qu'elle ne décroit jamais. Nous ne considérons donc pas la disparition de préfixes usurpés durant le mois en cours. Cette visualisation permet de mettre en évidence de manière efficace les instants où les usurpations se produisent. Sur chacune des figures, les usurpations de classe 1 sont représentées en violet, et

celles de classe 2 en bleu.

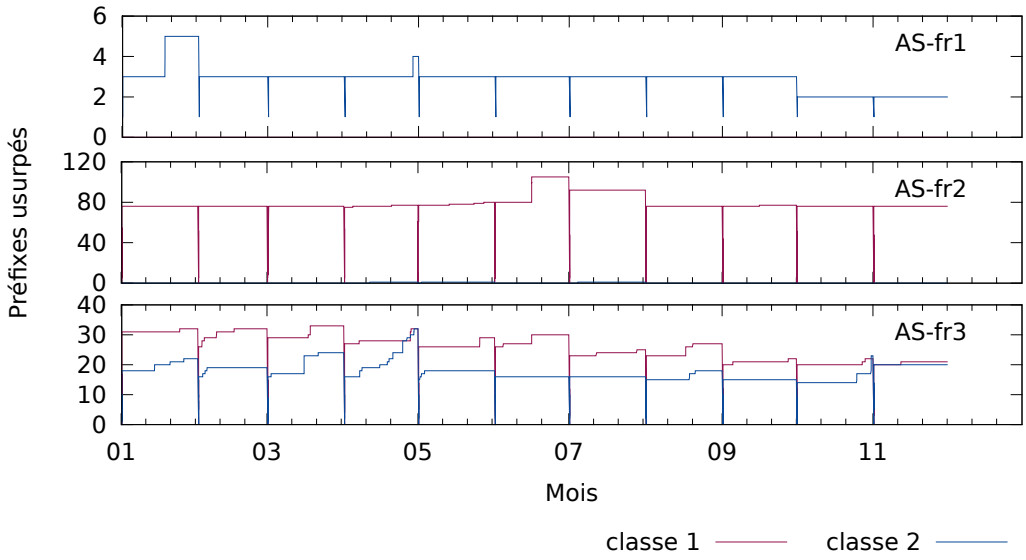

Figure 1.6 - Classes de préfixes usurpés par AS.

L'AS-fr1, figure 1.6, n'a pas subi d'usurpation de classe 1. Cependant, on peut très nettement voir qu'un certain nombre de préfixes lui appartenant sont annoncés par d'autres AS. Une étude approfondie des couples préfixes usurpés et AS usurpateurs a permis d'identifier que les AS usurpateurs sont en fait des fournisseurs de service de l'AS-fr1. Ces usurpations ne sont donc pas illégitimes, cependant la déclaration *d'objets route* auprès du RIPE fait défaut.

L'AS-fr2, figure 1.6, subit très peu d'usurpations de classe 2 en comparaison des usurpations de classe 1. L'AS-fr2 a ainsi délégué l'utilisation d'une partie de ses préfixes à ses clients sans en informer le RIPE. Il apparaît en effet que suite à des rachats, les *objets route* n'ont pas été mis à jour.

L'AS-fr3, figure 1.6, subit les deux classes d'usurpation de façon très franche. L'examen des préfixes usurpés et des AS usurpateurs indique qu'il s'agit pour la plupart de clients ou de sous-entités de l'opérateur gérées par l'AS-fr3. Il est important de souligner que les deux courbes décroissent au cours de l'année 2011. Les causes de cette décroissance ne sont actuellement pas connues mais peuvent être liées à deux phénomènes dont les effets se cumulent : une déclaration d'*objets route* plus cohérente et une diminution du nombre d'usurpations.

Après analyses, il semblerait que la plupart des usurpations mises en évidence par

notre algorithme sont légitimes pour tous les AS mais que les déclarations d'*objets route* n'ont pas été effectuées correctement. Comme il a été décrit précédemment, un transitaire strict ayant mis en œuvre des filtres d'annonces sur la base des *objets route* aurait rejeté tous les préfixes identifiés dans cette section. De par la visualisation adoptée, l'algorithme sera également capable de mettre en évidence des usurpations massives de préfixes par des AS illégitimes.

1.5 Conclusion et perspectives

Ce chapitre décrit le protocole BGP et présente différents indicateurs utilisés pour analyser la résilience de l'Internet français. Pour cette première édition du rapport annuel et afin de valider la méthodologie, nous avons limité cette étude à quatre AS français. À l'avenir, nous prévoyons l'étendre à davantage d'AS français afin d'offrir une analyse plus complète.

Tout d'abord, nous avons présenté des résultats concernant les *objets route* déclarés par les opérateurs. Cela nous a permis de mettre en évidence que ces déclarations ne sont pas systématiques et ne reflètent pas les préfixes réellement annoncés en BGP. Suite à des rachats, les *objets route* initiaux n'ont pas été mis à jour. Par conséquent, les préfixes se retrouvent annoncés par un AS qui n'est pas celui déclaré. De plus, cette étude a permis d'identifier les éventuels impacts liés au filtrage de préfixes sur la base des *objets route*. Ainsi, un grand nombre de préfixes d'un des quatre AS ne pourrait plus être visible si de tels filtrages étaient mis en place par un transitaire strict.

Nous avons également observé la structure de l'Internet français à l'aide de différents indicateurs comme le degré de connectivité des AS. Grâce à cette approche, nous avons pu établir une liste de 163 AS à forte concentration française, leurs interdépendances ainsi que les transitaires les plus utilisés. La journée mondiale IPv6, qui a eu lieu le 8 juin 2011, n'a pas eu le succès souhaité par les participants et les organisateurs. Peu de nouveaux préfixes IPv6 sont apparus lors de cette manifestation.

Finalement, nous nous sommes intéressés aux usurpations que subissent les quatre AS que nous avons choisi d'étudier. Deux grandes classes d'usurpation se sont ainsi détachées : celles effectuées par des AS directement connectés avec eux (appelées usurpations de classe 1), et celles effectuées par des AS qui ne le sont pas (usurpations de classe 2). Au cours de l'année 2011, les usurpations de classe 1 que nous avons mises en évidence sont, en grande partie, des annonces légitimes effectuées par des clients ; les AS étudiés n'ayant simplement pas fait les déclarations d'*objets route*.
Paradoxalement, l'étude fine des usurpations de classe 2 indique qu'elles sont également légitimes. Il s'agit dans la plupart des cas de fournisseurs de services de ces quatre AS auxquels des préfixes ont été délégués sans déclarer les *objets route*.

Les résultats présentés dans ce rapport sont une première étape vers une meilleure connaissance de l'Internet français et des indicateurs permettant de caractériser sa résilience de manière factuelle. À l'avenir, nous souhaitons élargir la portée de ce rapport en présentant de nouveaux indicateurs et en élargissant les résultats à l'ensemble des AS français. L'année 2012 amènera peut-être un déploiement plus franc de la technologie RPKI. Par conséquent, c'est un indicateur que nous allons tenter de mesu-

rer ces prochains mois. L'algorithme de détection des usurpations sera modifié pour prendre en compte les techniques de routage *anycast*. Les données exploitées dans ce rapport sont issues de données publiques et collectées à l'étranger. Afin d'obtenir une meilleure vision de l'Internet français, nous souhaitons mettre rapidement en place des collecteurs BGP en France. Cela nous permettra sans aucun doute d'améliorer la qualité des indicateurs que présentera le rapport de l'année 2012.

Chapitre 2

Résilience sous l'angle de l'infrastructure DNS

2.1 Introduction

Le système de noms de domaine (Domain Name System, DNS) est un système de nommage distribué et hiérarchique dont les deux objectifs essentiels sont d'associer à une adresse IP un nom plus lisible par les humains et, surtout, de fournir de la stabilité aux identificateurs [8] [1].

Cette stabilité des identificateurs est le principal objectif. En effet, l'adresse IP, dans la majorité des cas, dépend du Fournisseur d'Accès à Internet (FAI). Si on n'utilisait que les adresses IP, un changement d'hébergeur impliquerait de prévenir tous les utilisateurs, pour les informer de la nouvelle adresse. Le DNS permet au contraire de garder un identificateur qui ne change pas. Dans le cas d'un changement d'hébergeur, seul le responsable du domaine devra modifier l'adresse IP pointée par le domaine ; et grâce au DNS, ce changement sera transparent pour les utilisateurs.

La structure du DNS est illustrée dans la figure 2.1, page 32. Au sommet de la hiérarchie se trouve la racine représentée par un point « . » [2].

À chaque niveau de la hiérarchie se trouve un ou plusieurs nœuds de l'arbre DNS. L'arborescence issue d'un nœud donné est appelée domaine ; elle peut avoir à son tour des sous-domaines, et ainsi de suite. Si l'on considère les caractéristiques d'un nœud DNS uniquement à son niveau hiérarchique, c'est-à-dire, sans se préoccuper des éventuels sous-domaines qui en dérivent, on parle dans ce cas de zone DNS. Ce rapport ne tient pas compte de la différence subtile entre domaine (toute une arborescence à partir d'un nœud) et zone (seule la portion administrative autour de ce nœud). Par conséquent, ces deux termes seront désormais employés ici comme synonymes.

Pour chaque zone DNS, un ensemble de serveurs DNS permet de décrire les res-

1. Ainsi, l'adresse IP `2001:660:3003:2::4:20` correspond au nom de domaine `www.afnic.fr`.
2. À l'extrême droite du nom `www.afnic.fr`.

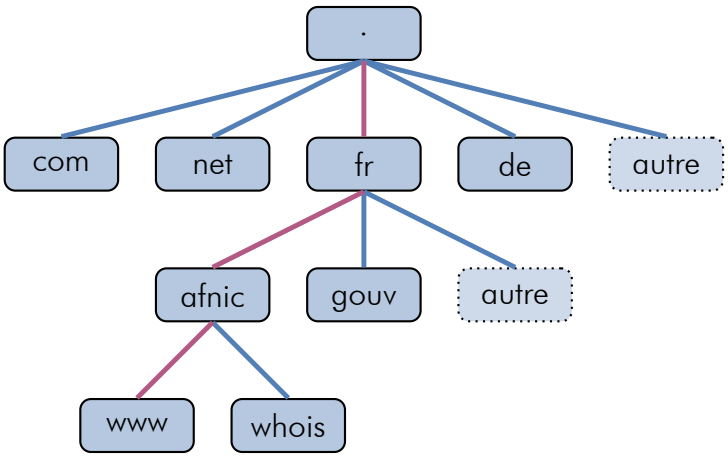

Figure 2.1 - Structure du DNS

sources qui lui sont directement attachées, ainsi que les éventuelles délégations directement au niveau en-dessous (zones déléguées). De tels serveurs sont appelés serveurs DNS faisant autorité pour la zone en question.

La résolution DNS est le mécanisme qui permet de récupérer une information, généralement une adresse IP, associée à un nom de domaine. La résolution DNS fait intervenir deux types de serveurs DNS comme l'illustre la figure 2.2 qui met en évidence des interactions numérotées :

- **un serveur récursif** (encore appelé serveur cache ou résolveur). C'est un serveur que la machine de l'utilisateur connaît et à qui elle soumet sa requête DNS [3] (interaction 1). Ce serveur va alors interroger le DNS en partant de la racine (interaction 2) et en suivant de proche en proche les points de délégation [4] jusqu'aux serveurs faisant autorité pour le nom de domaine objet de la requête (interactions 3-4). Enfin, le serveur récursif répond à la machine utilisateur (interaction 5) et garde en même temps en mémoire (fonction « cache ») les informations reçues, afin de les distribuer plus vite la fois suivante ;
- **des serveurs faisant autorité** pour des zones données, qui répondent au serveur récursif - soit, s'ils font effectivement autorité pour le nom de domaine demandé par la machine utilisateur, en lui retournant la réponse, soit en l'aiguillant vers d'autres serveurs à interroger faisant autorité et qui pourraient alors lui donner une meilleure réponse. Les serveurs faisant autorité sont généralement configurés volontairement sans la fonction cache : ils ne répondent que sur ce qu'ils savent en première main, c'est-à-dire avec des données provenant de leur propre base

3. Dans cet exemple de requête DNS, « IN A » signifie qu'on cherche le type d'adresse IPv4 de la classe IN (Internet), en pratique la seule classe utilisée.

4. La réponse « NS » indique une liste de serveurs de noms (« Name Server »).

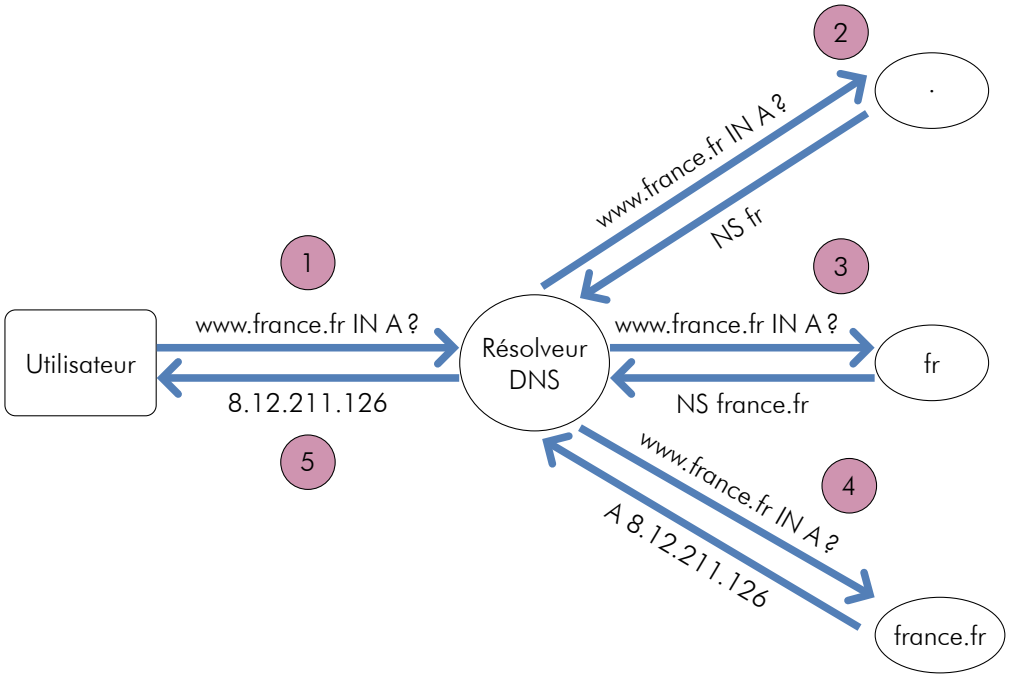

Figure 2.2 - Résolution DNS

de données.

2.1.1 Objectifs de ce chapitre

Nous cherchons à étudier différents indicateurs de résilience en lien avec le protocole DNS :

- la dispersion des serveurs de noms : selon le nombre d'opérateurs, les nombre d'AS, et les pays ;
- le nombre de serveurs DNS qui n'ont pas été corrigés pour la faille dite « Kaminsky » ;
- l'état du déploiement de certains protocoles comme IPv6 ou DNSSEC.

Pour ce faire, nous utilisons DNSwitness [9], plateforme générique développée par l'AFNIC permettant de réaliser des mesures via le DNS. Cette plateforme est multi-usages et capable de prendre en compte divers types de métriques. Les données brutes sont stockées dans une base de données afin d'étudier leur évolution dans le temps, notamment avec une vision long terme. Elle est conçue pour être distribuée librement et pour un usage flexible et adaptable au besoin.

DNSwitness a deux composantes :

- *DNSdelve*, pour les mesures actives ;

- *DNSmezzo*, pour les mesures passives.

DNSdelve prend en entrée une liste de zones (toutes les zones sous `.fr` par exemple, ou bien une liste spécialisée), effectue des requêtes DNS sur les zones en question, puis stocke les résultats extraits des réponses à ces requêtes dans une base de données.

DNSmezzo est, quant à lui, placé devant un serveur de noms (faisant autorité ou bien récursif), capture et analyse les requêtes DNS entrantes et/ou sortantes et place également le résultat dans la base de données.

2.1.2 Données utilisées

Toutes les mesures actives ont été faites en utilisant la zone `.fr`. Il faut se rappeler que `.fr` n'est pas toute la France. En effet, d'une part, des titulaires de noms de domaine établis en France peuvent utiliser des domaines de premier niveau autres que `.fr` (par exemple, `.com`, `.net`, `.org`, etc.), et de l'autre, des acteurs établis en dehors de la France peuvent choisir des noms de domaine en `.fr`[5].

Les données présentées ici proviennent de :

- l'Observatoire du marché des noms de domaine en France [10] pour le nombre de serveurs par zone. Cet observatoire vise, notamment, à fournir des clés d'analyse des facteurs déterminant le marché et des tendances de celui-ci ainsi qu'à identifier ses forces et ses faiblesses tout en proposant des recommandations ;
- la zone `.fr` telle qu'elle était en novembre et décembre 2011 (du point de vue du contenu du fichier de zone DNS) ;
- des campagnes de mesures faites par DNSdelve en novembre et décembre 2011, sur un échantillon de 10% de la zone `.fr` ;
- des campagnes de mesures faites par DNSmezzo en novembre et décembre 2011, sur les serveurs gérés par l'AFNIC et faisant autorité pour `.fr`. Ces mesures proviennent des 4 sondes actuellement en service sur les serveurs `c.nic.fr` (une sonde) et `d.nic.fr` (trois sondes placées à Paris, Lyon et Bruxelles). Le serveur `d.nic.fr` utilise la technique de l'*anycast*, permettant de répliquer le serveur DNS sur plusieurs sites physiques distincts (une instance par site), non connectés, qui répondent à la même adresse IP et assurent le même service. Cela augmente la résistance aux pannes et surtout aux attaques distribuées : l'attaquant ne verra pas toutes les instances *anycast* à la fois.

5. Peuvent enregistrer des noms de domaine sous `.fr` (et aussi sous `.re` et les autres domaines de premier niveau gérés par l'AFNIC), les personnes physiques ou morales établies sur le territoire de l'un des états membres de l'Union Européenne ou de celui de l'un des pays suivants : Islande, Liechtenstein, Norvège, Suisse.

2.2 Dispersion topologique des serveurs DNS faisant autorité

2.2.1 Description

Cet indicateur sert à apprécier la qualité de la répartition topologique et géographique des serveurs de noms pour l'ensemble des zones DNS déléguées sous la zone de référence (ici, `.fr`). Les éléments mesurés sont :

- le nombre de serveurs de noms par zone déléguée ;
- le nombre d'Autonomous System (AS) [6] différents par zone déléguée ;
- le nombre de pays différents par zone déléguée.

L'idée de base est de minimiser le risque qu'une panne arrête tous les serveurs de noms d'une zone. Ainsi, si une zone est servie par deux serveurs connectés au même bandeau électrique, une panne de la distribution électrique arrêtera les deux serveurs. Ils ne sont donc pas réellement indépendants.

La dispersion physique est importante mais n'est pas la seule à considérer. La dispersion au sens du routage IP en est une autre. Les serveurs de noms sont en effet interrogés en utilisant le protocole IP standard et dépendent donc d'un routage qui fonctionne. Si tous les serveurs de noms sont situés dans un réseau géré par un même opérateur et que ce réseau est rendu inaccessible depuis un point donné (à cause d'une panne de routage par exemple), la zone sera inaccessible, même si elle a beaucoup de serveurs de noms.

Selon le type de panne envisagé, ce sera l'une ou l'autre dispersion qui sera le facteur important pour la résilience. Ainsi, pour les pannes « physiques », le facteur important est en général la dispersion géographique. C'est évidemment plus complexe que cela : dans une région sismique comme la Californie, le facteur important n'est pas la distance mais la position relative aux failles géologiques. On ne met pas tous ses serveurs le long de la même faille. Malheureusement, nous n'avons pas accès à cette information. Pour certaines pannes « logiques » (erreur de configuration d'un routeur BGP, par exemple), c'est la dispersion selon plusieurs AS différents qui compte. Enfin, pour les pannes ayant une origine géographique, c'est le nombre de pays différents qui est pertinent.

La dispersion topologique est un indicateur de résilience significatif comme l'ont montré plusieurs pannes totales de domaines importants, dont ceux d'une grande entreprise française en juillet 2011 : tous les serveurs se trouvaient dans le même centre d'hébergement, et l'unique fibre optique du centre a été coupée.

6. Voir le chapitre 1 (BGP) pour la notion d'AS (en français, système autonome).

Avoir au moins deux serveurs faisant autorité est imposé par les recommandations de la RFC 1035 [11]. L'idée derrière cette exigence est que les deux serveurs ne tomberont pas en panne en même temps. Avec un seul serveur, toute panne est fatale. Mais leur dispersion topologique est une exigence plus récente (RFC 2182 [12] et 2870 [13]), issue de l'ingénierie de la résilience. Il s'agit d'éviter les Single Point Of Failure (SPOF), que ceux-ci soient un AS ou un pays. Certaines pannes peuvent paralyser tout un AS, par exemple une faute de frappe dans une *route-map* BGP (une option des routeurs permettant de filtrer les annonces d'un AS donné). Notons toutefois que la mesure externe ne suffit pas à détecter tous les SPOF. Pour reprendre l'exemple précédent, on ne peut pas détecter à distance si deux serveurs partagent la même alimentation électrique, ni s'ils sont administrés par un logiciel susceptible de changer leur configuration au même moment.

2.2.2 Méthodologie de mesure

Le nombre de serveurs de noms est directement déduit de la zone. Le nombre d'AS est obtenu en récupérant la liste des adresses IP des serveurs DNS faisant autorité, puis en obtenant le numéro d'AS via le service du Team Cymru [14], qui gère une base de correspondance entre les adresses IP et les numéros d'AS [7]. Le pays est connu en récupérant également la liste des adresses IP des serveurs de noms, puis par la base GeoIP de Maxmind [6], qui associe les adresses IP à des noms de pays. Ces bases GeoIP sont typiquement constituées à partir des données que les Regional Internet Registry (RIR) publient via le protocole whois.

Les pourcentages de serveurs de noms par pays ou par AS, présentées dans cette section sont en fait des « pourcentages de couples serveur et zone ». Un serveur gérant mille zones est ainsi comptabilisé mille fois, sa localisation topologique étant plus importante que celle d'un serveur qui ne sert qu'une zone.

2.2.3 Résultats et analyse

Nombre de serveurs de noms par zone

Dans le rapport 2011 de l'Observatoire du marché des noms de domaine en France [10], l'AFNIC explique que « la distribution du nombre de serveurs DNS associés aux noms de domaine `.fr` montre qu'une très large majorité des noms (plus de 83%) n'indiquent que deux serveurs DNS dans leur configuration, c'est-à-dire le minimum

7. Base générée automatiquement en regardant en temps réel les annonces BGP.

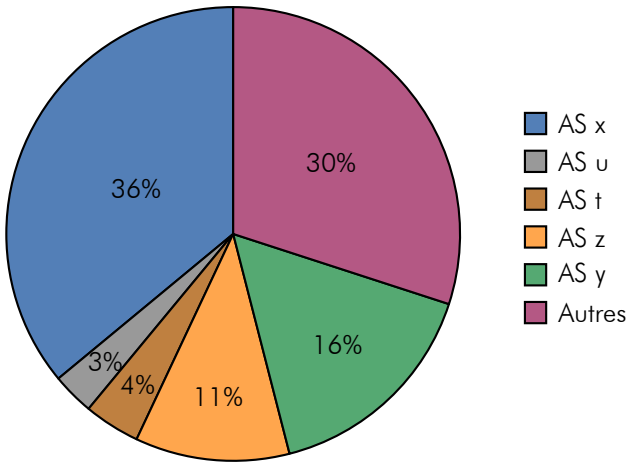

Figure 2.3 - Répartition par AS des serveurs de noms des zones sous .fr

exigé. Quelques domaines indiquent trois serveurs (14%), les configurations offrant plus de redondance étant beaucoup plus rares. Ces chiffres ont peu varié depuis 2010. Le nombre maximum de serveurs est de 8 et la moyenne se situe cette année encore à 2,2 serveurs par nom ».

Nombre d'AS par zone

Un maximum de sept AS par zone hébergée est atteint chez l'un des hébergeurs DNS professionnels, avec un AS distinct par adresse (sept serveurs de noms en tout pour chaque zone servie).

Le pourcentage de zones ayant plus de deux AS n'est que de 5%, alors que celui des zones avec un seul AS est de 80%. C'est certainement un des points de plus grande faiblesse de la résilience du DNS. Par ailleurs, le nombre moyen d'AS par zone est de 1,2.

Pour un point de vue différent sur les AS, la figure 2.3 montre les « parts de marché » des différents AS dans l'hébergement des serveurs de noms des zones sous `.fr`. Le but est de déterminer s'il existe des AS « importants » dont la panne affecterait sérieusement les zones sous `.fr`. On voit que deux AS hébergent les deux tiers des serveurs de noms sous `.fr`.

Nombre de pays par zone

La variété en termes de pays est à peine moindre : 2,6% de zones sont réparties dans

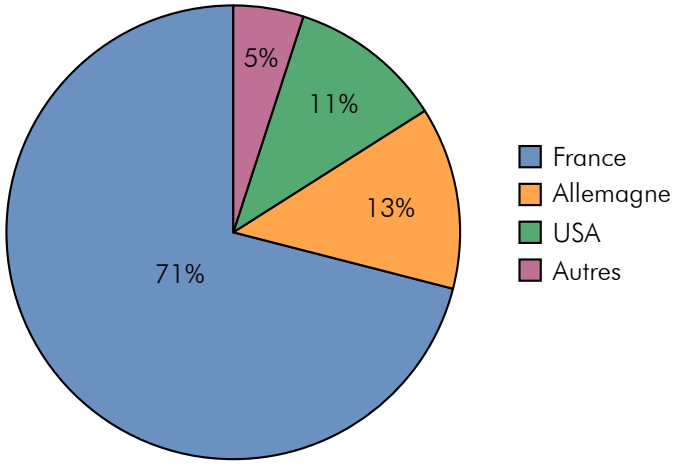

Figure 2.4 - Répartition par pays des serveurs de noms des zones sous .fr

plus de deux pays, 81% sur un seul, la moyenne étant de 1,2 et le maximum de 5 [8].

La figure 2.4 indique la répartition des serveurs de noms par pays au niveau de toute la zone `.fr`. Notons que ces chiffres supposent que tous les domaines sont équivalents, c'est-à-dire qu'un domaine détenu par un particulier pour héberger une page Web compte autant qu'un domaine auxquelles sont attachées des ressources d'intérêt national.

Cette figure montre que l'infrastructure DNS des zones sous `.fr` est assez auto-centrée sur la France : une coupure de toutes les liaisons avec les États-Unis, par exemple, n'aurait probablement pas de conséquences trop graves sur l'accessibilité des informations DNS contenues par ces zones.

8. Ce nombre est atteint par exemple par un domaine qui a des serveurs au Japon, aux États-Unis, en Suisse, en Grande-Bretagne et en Autriche.

2.3 Taux de résolveurs vulnérables à la faille Kaminsky

2.3.1 Description

La faille Kaminsky, annoncée en 2008, exploite une faiblesse du protocole DNS qui permet un empoisonnement du cache DNS, c'est-à-dire l'injection de fausses informations dans un serveur cache. Elle peut donc être exploitée pour détourner les utilisateurs, par exemple vers un site Web de hameçonnage où ils seront incités à fournir des données de connexion qui seront utilisées par la suite par les fraudeurs en usurpant l'identité des utilisateurs ainsi piégés.

La vulnérabilité était connue depuis longtemps [15] mais l'idée de Dan Kaminsky a rendu l'utilisation de cette faille bien plus rapide que ce que l'on pensait possible. Les serveurs vulnérables peuvent ainsi être empoisonnés en quelques minutes, en n'utilisant que des programmes déjà disponibles sur l'Internet.

Deux solutions à cette faille étaient proposées en 2008 : une à court terme appelée Source Port Randomization (SPR), qui ajoute de l'entropie à la requête en rendant aléatoire la sélection du port source ; et l'autre à long terme, DNSSEC, qui permet de signer numériquement les enregistrements DNS. La première solution a été mise en œuvre dans la plupart des résolveurs DNS ; certains, comme Unbound, l'utilisaient déjà.

2.3.2 Méthodologie de mesure

À partir des données fournies par DNSmezzo, nous cherchons à mesurer le nombre de ports sources différents utilisés par les résolveurs qui interrogent les serveurs faisant autorité pour `.fr`. Le nombre minimum de dix est un seuil jugé acceptable du point de vue statistique, pour permettre de déduire que le résolveur fait suffisamment varier le port source pour ses requêtes ou non ; seules les données des serveurs envoyant au moins dix requêtes sont donc conservées.

2.3.3 Résultats et analyse

L'étude montre que 9 à 10% des résolveurs utilisent trop peu de numéros de ports sources différents ; souvent, ils en utilisent un seul. Ce chiffre dépend du serveur fai-

sant autorité (pour `.fr`) étudié ; l'un des serveurs en voit nettement plus pour des raisons inconnues.

Ces résolveurs vulnérables sont à l'origine de 5 à 8% des requêtes reçues par les serveurs faisant autorité pour `.fr`. On peut en déduire que ces résolveurs envoient moins de requêtes que la moyenne. Mais ils ne représentent pas un trafic négligeable pour autant.

Notons que le taux de résolveurs vulnérables était de 25% quelques mois après l'annonce de la faille Kaminsky. La mise à jour continue donc, très lentement, probablement uniquement lorsque les machines physiques sont remplacées, profitant ainsi d'un « rafraîchissement » naturel du logiciel.

Voici un exemple, sur des données de test, des résultats du programme utilisé :

```
192.0.2.20: 0.0014 (1 port, 735 requests)
198.51.100.8: 0.0022 (1 port, 459 requests)
2001:db8:ba:ffe::9:11 0.0040 (1 port, 250 requests)
203.0.113.2: 0.0045 (1 port, 222 requests)
```

Certains serveurs analysés peuvent ne pas être des vrais résolveurs mais un étudiant expérimentant *dig* [9]. Toutefois, l'analyse des requêtes semble indiquer que, la plupart du temps, il s'agit bien de vrais résolveurs vulnérables.

9. Un outil logiciel courant, faisant partie de la distribution BIND et permettant de tester des serveurs DNS.

2.4 Taux de pénétration de DNSSEC

2.4.1 Description

DNSSEC est une technique d'authentification des enregistrements DNS, reposant sur la cryptographie. Le principe est de signer les enregistrements avant diffusion. Un résolveur qui gère DNSSEC pourra ainsi les valider, s'assurer de leur authenticité, quel que soit le chemin par lequel il les a reçus. Le dit résolveur doit connaître une clé de départ (typiquement celle de la racine) ; il trouve les clés suivantes dans le DNS, en parcourant une série de délégations signées (appelée chaîne de confiance) et en s'appuyant sur une série des enregistrements nommés DS (*Delegation Signer*).

Il y a plusieurs indicateurs ici :

- pourcentage de zones signées avec DNSSEC ;
- pourcentage de zones ayant un enregistrement Delegation Signer (DS) dans `.fr`. Un DS traduisant la signature de la clé de la zone en question par celle de sa zone parente, le `.fr`, établissant ainsi une chaîne de confiance.

La différence entre le pourcentage de zones signées et le pourcentage de zones possédant DS dans `.fr` vient des zones signées à titre expérimental, pas encore stabilisées, et surtout des zones dont le Bureau d'Enregistrement (BE [10]) n'offre pas la possibilité de soumettre un DS au niveau de `.fr`. C'est le cas aujourd'hui de la majorité des BE en France.

DNSSEC n'est pas un facteur de résilience en soi. Cependant, compte tenu du caractère désormais normatif de déployer les extensions de sécurité qu'il apporte [11], le faire sans respecter les bonnes pratiques, diminue la résilience du service de résolution DNS avec validation DNSSEC. En effet, une erreur de mise en œuvre, de configuration, ou une négligence provoquant l'expiration de clés DNSSEC, peut entraîner un échec de résolution sur les résolveurs validants, et par conséquent une inaccessibilité du service visé après résolution DNS.

2.4.2 Méthodologie de mesure

Les données sur le nombre de DS sont simplement tirées de la base de données de `.fr`. Celles sur le nombre de zones signées, proviennent de DNSdelve et donc de mesures actives.

10. En québécois, registraire.
11. Aujourd'hui, il n'y a guère plus de débat sur son intérêt/utilité mais plutôt sur le moment de le faire pour chaque acteur concerné.

2.4.3 Résultats et analyse

En examinant la zone `.fr`, on constate qu'actuellement, il y a 33 noms de domaine auxquels sont associés un ou deux enregistrements DS sur un total de 2 131 775 noms de domaine dans la zone `.fr`. Ce nombre a peu évolué depuis le mois d'août 2011. Il est à noter que c'est à partir du 19 avril 2011 que les enregistrements DS des zones signées ont pu être insérés au niveau de la zone `.fr`.

Inversement, le module DNSSEC de DNSdelve a permis de voir qu'il y a 14 zones signées, lors du dernier lancement qui a utilisé un taux d'échantillonnage à 10%. Il pourrait donc, statistiquement, y avoir de l'ordre de 140 zones signées (mais uniquement 33 zones avec un DS dans la zone parente).

2.5 Taux de pénétration d'IPv6

2.5.1 Description

Le taux de pénétration d'IPv6 est très difficile à définir dans l'absolu, compte tenu de la diversité de domaines dans lesquels on peut observer l'évolution du déploiement de cette nouvelle version d'IP. Cependant, vu sous l'angle du DNS, on peut tenter de caractériser l'évolution de la pénétration d'IPv6 par les indicateurs suivants :

- le nombre de zones ayant au moins un serveur de noms et/ou un serveur Web et/ou un serveur de messagerie avec une adresse IPv6 ;
- le pourcentage de requêtes DNS reçues au-dessus d'IPv6 ;
- le type d'adresse demandé (A pour IPv4 ou AAAA pour IPv6).

Précisons tout d'abord que le niveau de pénétration d'IPv6 ne peut être considéré comme un facteur de résilience en soi. Cependant, les techniques de déploiement en double pile IPv4-IPv6 (appelée « *dual-stack* ») apparaissent comme une condition nécessaire dans plusieurs environnements pour assurer une transition fluide. La résilience des infrastructures et des services IP peut être affectée positivement ou négativement selon la qualité du déploiement d'IPv6 et aussi de celui de la maintenance de l'existant en IPv4. Par exemple, publier dans le DNS une nouvelle entrée IPv6 (AAAA) pour un service, au côté de celle en IPv4 (A), sans s'assurer au préalable que le service est bien opérationnel en IPv6, rend le service au mieux dégradé (si le client a la possibilité de se rabattre en IPv4), et au pire inaccessible (dans le cas contraire). À l'inverse, un déploiement d'IPv6 dans les règles de l'art peut représenter un facteur supplémentaire de résilience pour un service existant en IPv4, dans le cas où ce service est momentanément inaccessible en IPv4 (par exemple à cause d'un problème de routage IPv4).

2.5.2 Méthodologie de mesure

Le nombre de zones ayant des adresses IPv6 est mesuré activement par le module IP de DNSdelve. Celui-ci fait une requête de type AAAA (adresse IPv6) sur les noms `www.LEDOMAINE.fr` et `LEDOMAINE.fr`. Le pourcentage de requêtes transportées sur IPv6, lui, est mesuré passivement par DNSmezzo et vérifié avec l'outil DSC (logiciel de statistique de trafic DNS temps-réel, très utilisé par les opérateurs de serveurs DNS) sur les serveurs administrés directement par l'AFNIC. Il en va de même pour le type des données demandé. On notera que les résultats sont *a priori* biaisés en faveur d'une clientèle française, vu la localisation des serveurs administrés par l'AFNIC.

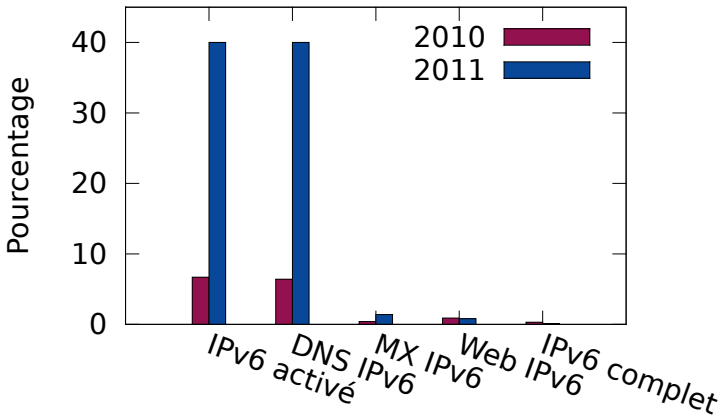

Figure 2.5 - Évolution de la pénétration d'IPv6 entre 2010 et 2011

2.5.3 Résultats et analyse

Dans les zones DNS déléguées sous .fr

DNSdelve nous indique les éléments suivants :

- le taux global de zones ayant au moins un serveur DNS, Web ou courrier [12] répondant en IPv6 est de 40% (dans ces cas là on dit que « IPv6 est activé ») ;
- le taux des zones ayant tous leurs serveurs configurés (DNS, Web et courrier) pour IPv6 est très faible : 0,008% (dans ces cas, on dit que « IPv6 est complet ») ;
- ce sont avant tout les serveurs DNS qui font de l'IPv6, puisque leur taux est le même que le taux global donné plus haut, soit 40% ;
- les serveurs de courrier font très rarement de l'IPv6. Seuls 1,4% d'entre eux en font ;
- quant aux serveurs Web, ce sont les serveurs les moins bien lotis, avec un taux de 0,8%.

Il est bon de rappeler que les chiffres précédents sont des taux relatifs à la taille de la zone `.fr` (nombre de zones déléguées) qui, elle-même est variable, et a augmenté de 23% en 2009 et 18% en 2010 [13]. L'évolution dans le temps de ces chiffres se trouve sur la figure 2.5. Par ailleurs, la croissance assez marquée d'IPv6 en 2011 est due à l'activation d'IPv6 sur quelques serveurs chez des hébergeurs DNS accueillant un grand nombre de zones.

12. Seuls ces types de services sont examinés aujourd'hui.
13. En novembre 2011, la zone `.fr` comptait près de 2,2 millions de zones déléguées.

Type	Description	Proportion
A	Adresse IPv4	0,804
MX	Serveur de courrier	0,083
AAAA	Adresse IPv6	0,067
NS	Serveurs de noms	0,017
TXT	Texte libre (utilisé par exemple pour SPF)	0,007
*	Tous les enregistrements	0,006
DS	Signature DNSSEC d'une délégation	0,005
SRV	Recherche d'un service	0,002
SOA	Autorité de la zone	0,002
A6	A6 (Abandonné depuis longtemps mais toujours répandu)	0,002

Table 2.1 - Proportion de requêtes DNS par type de données demandé

Dans les requêtes

Rappelons qu'il y a deux éléments dans une requête DNS pour lesquels IPv6 peut être pris en considération : le transport - le protocole utilisé pour poser la question - et le type, le fait que la question soit pour un A (adresse IPv4) ou pour un AAAA (adresse IPv6). Ces deux éléments sont totalement indépendants.

Pour les serveurs faisant autorité pour `.fr` et étant directement administrés par l'AFNIC, environ 2,2% des requêtes sont transportées en IPv6. Ce chiffre est en progression régulière (il était de moins de 1% jusqu'en 2009) mais reste très faible.

Pour donner une idée de ce que cela représente, le serveur `d.nic.fr` voit entre 20 et 50 requêtes par seconde en IPv6 contre entre 600 et 1600 en IPv4.

Il faut se rappeler que les clients des serveurs de l'AFNIC ne sont pas des machines classiques (d'utilisateurs finaux) mais des résolveurs. On peut imaginer que ces résolveurs, gros serveurs gérés par des professionnels (FAI par exemple), utilisent plus souvent le protocole IPv6 que les machines terminales.

Quant aux types de données demandés, il y a toujours huit à douze fois plus de requêtes A que AAAA. Pour des raisons non encore élucidées, le pourcentage de AAAA dépend sérieusement du serveur interrogé. Et ce chiffre, lui, ne semble pas changer depuis 2009 : il reflète des choix de la machine terminale, contrairement au transport, qui reflète un choix du résolveur.

Le tableau 2.1 présente les types de données pour lesquels il y a plus de 1 ‰ des requêtes [14]. Il permet de constater qu'il y a encore de grandes disparités entre les nombres de requêtes concernant les adresses IPv4 et celles concernant les adresses IPv6.

14. La part des MX varie énormément d'un jour à l'autre, selon qu'il y a une campagne de *spam* en cours ou pas.

2.6 Conclusion et perspectives

Cette étude menée à travers le prisme du DNS montre que la résilience des zones sous `.fr` pourrait être améliorée. On trouve encore trop de zones « importantes » qui n'ont pas assez de serveurs de noms, et dont tous les serveurs sont au même endroit physique. Plus précisément :

- pour la majorité des zones sous `.fr`, le nombre des serveurs de noms est insuffisant : il pourrait y avoir davantage de serveurs (actuellement, 2,2 par zone en moyenne), et surtout des serveurs répartis sur davantage d'opérateurs (actuellement, seulement 1,2 en moyenne par zone) ;
- des années après la publication d'une importante vulnérabilité, la faille Kaminsky, et de sa correction, 10% des serveurs de noms font toujours tourner des programmes vulnérables ;
- les déploiements de certaines nouvelles techniques, nécessaires à l'Internet du futur, comme IPv6 (40% des zones DNS, mais moins de 1% des serveurs Web) et surtout DNSSEC (pratiquement pas de zones signées), restent très faibles.

Au niveau de l'infrastructure DNS, la situation en France est aujourd'hui acceptable mais rien ne garantit que cela soit toujours le cas à l'avenir. Compte tenu du caractère critique de l'Internet dans notre vie, il est souhaitable que tous les acteurs s'investissent dans une amélioration de sa résilience, notamment sur les aspects DNS (meilleure dispersion topologique, déploiement de DNSSEC et d'IPv6 de manière conforme aux bonnes pratiques). À l'avenir, de nouveaux indicateurs seront mesurés afin d'obtenir une meilleure vision de l'Internet en France. Tout d'abord, les configurations des serveurs de la zone `.fr` seront testées à l'aide de l'outil Zonecheck [16] de l'AFNIC. Concernant DNSSEC, il est prévu de mesurer le nombre de clés dans la zone et leur algorithme. La diversité des souches logicielles différentes utilisées pour une zone ou pour un site sera également prise en compte (on parle souvent de « diversité génétique »). Cela permettra, par exemple, d'appréhender les conséquences des bogues sur les différents logiciels.

Conclusion générale

Ce rapport présente les premiers résultats de l'observation de la résilience de l'Internet français sous l'angle des protocoles BGP et DNS. Pour chacun de ces deux protocoles, des indicateurs pertinents pour la résilience ont été rigoureusement définis, mesurés et enfin interprétés.

Les conclusions des analyses introduites dans ce rapport peuvent être utilisées de manière indépendante pour améliorer la résilience de l'Internet français. Plusieurs axes d'amélioration à court terme, découlant de bonnes pratiques de déploiement, sont ainsi envisageables. En particulier, vu sous l'angle BGP, il est souhaitable de procéder à une déclaration systématique et cohérente des *objets route* auprès du RIPE-NCC. Sous l'angle DNS, il est également souhaitable d'obtenir une plus grande dispersion des serveurs de noms faisant autorité au sein d'AS différents.

Par ailleurs, concernant le protocole IPv6, les analyses présentées dans ce rapport indiquent que les déploiements et les usages demeurent peu nombreux. À part les serveurs DNS eux-mêmes, pour lesquels il y a eu une croissance remarquable sur les deux dernières années, les autres serveurs des domaines `.fr` utilisent peu IPv6. De même, une proportion négligeable des requêtes reçues par l'AFNIC sont faites en IPv6. Sous l'angle de BGP, le même phénomène est observé : la plupart des AS français identifiés ne supportent pas IPv6. Ces constats indiquent qu'une adoption rapide du protocole IPv6 n'est pas certaine, et soulèvent des questions quant à la maturité des implantations du protocole dans les équipements et les logiciels.

Au cours de l'année 2011, différents incidents et avis de sécurité [17, 18, 19] ont concerné les protocoles DNS et BGP ainsi que leurs mises en œuvre. Ces événements montrent qu'il peut être assez risqué de reposer sur un unique équipementier ou logiciel dans une infrastructure. Cependant, la multiplication des fournisseurs peut rendre l'exploitation plus compliquée. Une alternative à cette diversification passe par la confiance accordée aux équipements, la qualité de leurs configurations, et l'expertise des administrateurs.

Le rapport 2011 a donné lieu à un ensemble d'indicateurs permettant d'appréhender ce qui caractérise la résilience de l'Internet sur le plan technique. Au cours de l'année 2012, l'observatoire souhaite étudier les attaques DNS perçues par les serveurs caches, et mettre en place des collecteurs BGP en France. Ces deux initiatives per-

mettront d'obtenir des données plus fines afin d'améliorer la vision de la résilience de l'Internet français que fournira le rapport 2012. Les organismes voulant participer à cette initiative peuvent s'adresser à l'ANSSI et l'AFNIC.

Bibliographie

[1] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)." RFC 4271 (Draft Standard), Jan. 2006. Updated by RFCs 6286, 6608.

[2] Wikipedia, "Registre Internet Régional." <http://fr.wikipedia.org/wiki/Registre_Internet_régional>.

[3] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing." RFC 6480 (Informational), Feb. 2012.

[4] D. Dugal, C. Pignataro, and R. Dunn, "Protecting the Router Control Plane." RFC 6192 (Informational), Mar. 2011.

[5] RIPE, "Routing Information Service (RIS)." <http://www.ripe.net/data-tools/stats/ris/>.

[6] MaxMind, "GeoIP | IP Address Location Technology." <http://www.maxmind.com/app/ip-location>.

[7] D. McPherson, R. Donnelly, and F. Scalzo, "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services." RFC 6382 (Best Current Practice), Oct. 2011.

[8] Stéphane Bortzmeyer, "Pourquoi le DNS ?." <http://www.bortzmeyer.org/pourquoi-le-dns.html>.

[9] AFNIC, "DNSwitness." <http://www.dnswitness.net/>.

[10] AFNIC, "Observatoire 2011 du marché des noms de domaine en France." <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/5381/show/l-afnic-publie-l-edition-2011-de-l-observatoire-du-marche-des-noms-de-domaine.html>.

[11] P. Mockapetris, "Domain names - implementation and specification." RFC 1035 (Standard), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.

[12] R. Elz, R. Bush, S. Bradner, and M. Patton, "Selection and Operation of Secondary DNS Servers." RFC 2182 (Best Current Practice), July 1997.

[13] R. Bush, D. Karrenberg, M. Kosters, and R. Plzak, "Root Name Server Operational Requirements." RFC 2870 (Best Current Practice), June 2000.

[14] Team CYMRU Community Services, "IP TO ASN MAPPING." <http://www.team-cymru.org/Services/ip-to-asn.html>.

[15] Stéphane Bortzmeyer, "Comment fonctionne la faille Kaminsky ?." <http://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>.

[16] AFNIC, "ZoneCheck." <http://www.zonecheck.fr>.

[17] CERTA-2011-AVI-381, "Multiples vulnérabilités dans Bind." <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-381/index.html>.

[18] CERTA-2011-AVI-645, "Vulnérabilité dans ISC BIND." <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-645/index.html>.

[19] CERTA-2011-AVI-619, "Vulnérabilité dans Juniper." <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-619/CERTA-2011-AVI-619.html>.

Acronymes

AFNIC	Association Française pour le Nommage Internet en Coopération
ANSSI	Agence nationale de la sécurité des systèmes d'information
AS	Autonomous System
BE	Bureau d'Enregistrement
BGP	Border Gateway Protocol
CGN	Carrier Grade NAT
DNS	Domain Name System
DNSSEC	DNS SECurity extensions
DoS	Denial of Service
DS	Delegation Signer
DSC	DNS Statistics Collector
FAI	Fournisseur d'Accès à Internet
NAT	Network Address Translation
RIR	Regional Internet Registry
SPOF	Single Point Of Failure
SPR	Source Port Randomization
TLD	Top Level Domain

À propos de l'AFNIC

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

L'AFNIC se positionne également comme fournisseur 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.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Juin 2012

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr