Résilience de l'Internet français

2014

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

Document réalisé par l'ANSSI avec la participation de l'Afnic.

Recherche et rédaction par : François Contat, Vincent Levigneron, Pierre Lorinquer, Florian Maury, Samia M'timet, Mohsen Souissi, Michal Toma, Guillaume Valadon, et Nicolas Vivet.

L'équipe de rédaction remercie les membres de l'observatoire ainsi que les relecteurs pour leurs commentaires et remarques qui ont enrichi ce rapport.

Document mis en page à l'aide de LaTeX. Figures réalisées avec les outils TikZ et PGFPlots.

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

rapport.observatoire@ssi.gouv.fr

Table des matières

Synthèse

Depuis 2011, l'observatoire de la résilience de l'Internet français étudie les technologies critiques au bon fonctionnement de l'Internet en France. Afin d'appréhender les dépendances des activités économiques et sociales nationales vis-à-vis de l'étranger, l'observatoire se focalise sur l'Internet français, un sous-ensemble de l'Internet en France ne prenant pas en compte les acteurs étrangers.

La résilience est définie comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Elle peut être caractérisée par des indicateurs mesurables. Certains sont directement issus de règles d'ingénierie, appelées bonnes pratiques, définies par la communauté technique et scientifique.

Rédigé par l'ANSSI [1] avec la participation de l'Afnic [2], ce quatrième rapport analyse la résilience en étudiant deux protocoles essentiels au fonctionnement de l'Internet. Le premier, BGP [3], permet d'acheminer des données à l'aide d'annonces de routage. Le second, DNS [4], fournit la correspondance entre un nom de domaine et une adresse IP.

En 2014, l'observatoire a identifié de nombreuses activités malveillantes utilisant BGP comme vecteur pour détourner du trafic. Concernant le protocole IPv6, deux faits remarquables sont survenus : l'augmentation de la concentration des interconnexions, et l'inertie des nouveaux déploiements perçue à travers le DNS. Le nouvel indicateur portant sur la messagerie électronique a, par ailleurs, mis en évidence un nombre insuffisant de relais de messagerie des zones déléguées sous `.fr`.

Au regard des analyses concernant l'année 2014, l'observatoire renouvelle ses encouragements aux acteurs de l'Internet concernant l'appropriation des bonnes pratiques d'ingénierie admises pour les protocoles BGP [1] et DNS [2]. D'autre part, l'observatoire énonce les recommandations suivantes :

- **surveiller les annonces de préfixes**, et se tenir prêt à réagir en cas d'usurpation ;
- **diversifier le nombre de serveurs SMTP et DNS** afin d'améliorer la robustesse de l'infrastructure ;
- **appliquer les bonnes pratiques** pour limiter les effets des pannes et des erreurs d'exploitation ;
- **poursuivre les déploiements** d'IPv6, de DNSSEC, et de la RPKI, afin de développer les compétences et d'anticiper d'éventuels problèmes opérationnels.

1. Agence nationale de la sécurité des systèmes d'information.
2. Association Française pour le Nommage Internet en Coopération.
3. Border Gateway Protocol.
4. Domain Name System.

Présentation de l'observatoire

L'Internet est une infrastructure essentielle pour les activités économiques et sociales aux échelles mondiale, nationale, et locale. Une panne majeure affecterait considérablement la bonne marche de la France et de son économie. De plus, le fonctionnement de l'Internet dans son ensemble est souvent méconnu et peut être perçu comme un système opaque, géré par des acteurs dont les rôles sont mal identifiés. Malgré l'importance de cette problématique, il n'existait pas d'organisme chargé d'étudier les risques de dysfonctionnement de l'Internet au niveau national.

Mis en place sous l'égide de l'ANSSI en 2011, l'observatoire de la résilience de l'Internet français vise ainsi à améliorer la connaissance de celui-ci en étudiant les technologies critiques à son bon fonctionnement. Un de ses objectifs est d'augmenter la compréhension collective de l'Internet français afin d'en avoir une vision cohérente et la plus complète possible. Cela permet notamment d'identifier les interactions entre les différents acteurs concernés.

De par sa nature, l'Internet est international et ne possède pas de frontière. Il est cependant possible de définir l'Internet en France comme l'ensemble des acteurs français et internationaux exerçant une activité en lien avec les technologies de l'Internet au sein du territoire. Dans le cadre de ses études, l'observatoire se focalise sur l'Internet français, un sous-ensemble de l'Internet en France, qui n'inclut pas les acteurs étrangers. L'étude de l'Internet français permet de mieux comprendre les interdépendances des activités économiques et sociales françaises vis-à-vis de sociétés ou d'organismes étrangers.

La résilience est, quant à elle, définie comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Une extension naturelle en 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, la résilience et la robustesse de l'Internet peuvent être caractérisées par un ensemble d'indicateurs techniques mesurables. Certains sont directement issus de règles d'ingénierie, appelées bonnes pratiques, définies par la communauté technique et scientifique.

La mission de l'observatoire de la résilience de l'Internet français est également de définir et de mesurer des indicateurs représentatifs de la résilience, et de rendre leurs résultats publics. Il associe à cette démarche les acteurs de l'Internet français afin d'augmenter l'efficacité du dispositif et de favoriser une adoption la plus large possible des bonnes pratiques.

Introduction

Cette quatrième édition du rapport de l'observatoire fournit des analyses concernant la mise en œuvre des protocoles BGP et DNS. Par souci de concision, et afin de renouveler le contenu, ce nouveau rapport présente une synthèse des analyses pour les indicateurs déjà étudiés dans les éditions précédentes, et détaille les éléments marquants de l'année 2014. Le rapport 2013 constitue ainsi la référence en ce qui concerne les descriptions et les méthodologies des indicateurs techniques récurrents.

En 2014, l'observatoire s'est attaché à améliorer ses outils afin d'augmenter le volume de données traitées, tout en facilitant leur étude. Pour ce faire, des technologies de type *Big Data* [3] ont été employées pour répartir le stockage et les traitements sur plusieurs nœuds de calcul. Désormais, l'ensemble des archives BGP mises à disposition par le projet RIS [5] est pris en compte, multipliant par trois la quantité d'informations gérée. Cette nouvelle infrastructure [4] permet ainsi d'analyser les quelques 50 000 AS qui constituent l'Internet. Par ailleurs, de nouveaux outils ont été développés pour étudier les serveurs de courriers électroniques sous l'angle du protocole DNS.

Jusqu'alors, l'observatoire n'était pas en mesure de traiter les données BGP en temps réel. Par conséquent, la détection des usurpations de préfixes était effectuée a posteriori. Pour pallier ce manque, l'observatoire a donc optimisé son traitement des annonces BGP afin de détecter les usurpations au plus tôt, et d'effectuer des mesures actives pour identifier des redirections de trafic. Il s'agit d'une avancée importante qui permet de mieux comprendre et appréhender les effets des usurpations de préfixes.

En marge des travaux présentés dans ce rapport, l'observatoire et ses partenaires publient des guides, notamment sur la prévention des attaques DDoS [6] [5] et le protocole BGP [1] afin d'améliorer la compréhension des risques, et de limiter leurs impacts éventuels.

À retenir

Les opérateurs désireux d'obtenir des informations détaillées, concernant les indicateurs BGP, peuvent solliciter des rapports individualisés.

5. Routing Information Service.
6. Distributed Denial of Service.

Chapitre 1

Résilience sous l'angle du protocole BGP

1.1 Introduction

1.1.1 Fonctionnement du protocole BGP

Chacun des opérateurs de l'Internet gère des ensembles d'adresses IP[1] contiguës, appelés préfixes, qu'il peut diviser pour ses propres besoins ou ceux de ses clients. Afin de constituer l'infrastructure de l'Internet, les opérateurs se connectent entre eux à l'aide de BGP [6]. L'objectif de ce protocole est d'échanger des préfixes entre deux opérateurs qui sont alors appelés AS[2] et qui sont identifiés par un numéro unique.

Chacun des AS informe son interlocuteur ou pair qu'il a la possibilité d'acheminer le trafic à destination de ses préfixes. Les interconnexions se divisent en deux catégories :

- **le peering :** accord où chaque pair annonce à l'autre les préfixes qu'il gère. Par exemple, si un fournisseur d'accès et un diffuseur de contenu passent un accord de *peering*, ils s'échangeront leur trafic directement ;
- **le transit :** accord commercial entre un client et son opérateur de transit. En pratique, le client annonce ses préfixes à son opérateur pour qu'il les propage. Ce dernier lui annonce en retour le reste des préfixes constituant l'Internet.

Dans une interconnexion BGP, chaque pair associe un `AS_PATH`, ou chemin d'AS, aux préfixes qu'il annonce. Dans la figure 1.1, le routeur de l'AS65540 a appris l'`AS_PATH` `64510 64500` pour le préfixe 192.0.2.0/24. Pour joindre l'adresse IP 192.0.2.1, un paquet au départ de l'AS65540 traversera l'AS64510 avant d'arriver à l'AS64500. 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 responsable de l'annonce des routes. Dans la figure 1.1, le routeur de l'AS65550 possède deux routes pour joindre le préfixe 192.0.2.0/24. L'une a été apprise via une interconnexion de peering (en bleu), et l'autre via une interconnexion de transit (en violet). En l'absence d'autre information, le chemin d'AS le plus court détermine la route utilisée. Dans cet exemple, il s'agit du lien de peering.

Il n'existe aucune méthode d'authentification robuste des annonces de préfixes. Par conséquent, un AS malveillant peut annoncer un préfixe appartenant à un autre AS.

1. Internet Protocol.
2. Autonomous System.

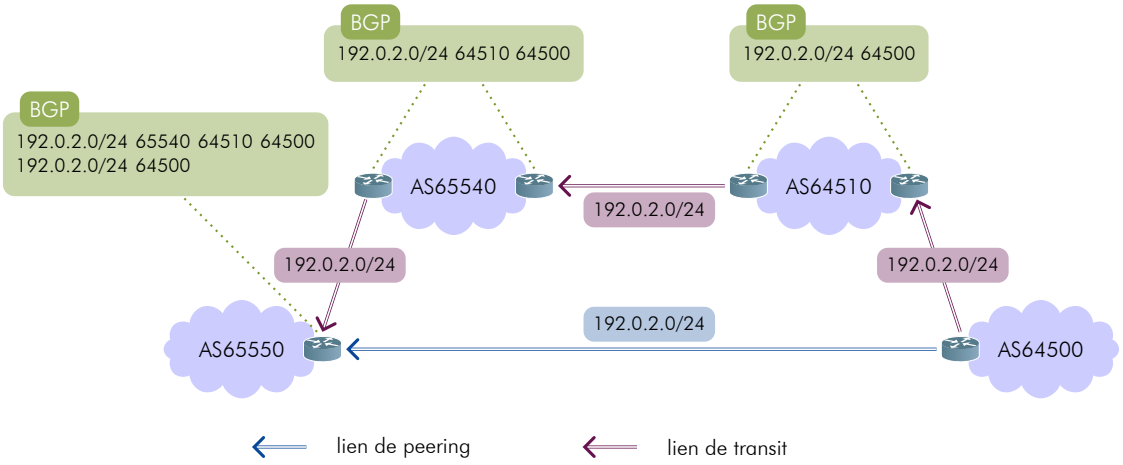


Figure 1.1 – Exemple de chemins d'AS sur des liens de transit et peering

C'est ce que l'on appelle une usurpation de préfixe [3]. Les conséquences peuvent être plus ou moins graves selon l'annonce qui est faite. Le réseau victime peut ainsi devenir injoignable pour tout ou partie de l'Internet. Ce type d'incident peut également entraîner une redirection du trafic destiné au réseau victime vers le réseau ayant usurpé les préfixes.

1.1.2 Les objets route

Les bonnes pratiques [1] veulent qu'un organisme déclare, dans la base `whois`, les préfixes qu'il annonce en BGP. Ces déclarations doivent être effectuées par l'intermédiaire d'objets `route` et sont stockées dans les serveurs d'un IRR [4]. Ce service est opéré par chaque RIR [5], dont le RIPE-NCC [6] pour l'Europe. Un objet `route` permet d'identifier clairement les AS susceptibles d'annoncer les préfixes de l'organisation.

```
route:          198.18.7.0/24
descr:          Prefixe d'exemple
origin:         AS64496
mnt-by:         MNTNER-RO-EXEMPLE
```

Figure 1.2 – Exemple d'un objet `route`

L'objet `route` de la figure 1.2 indique que le préfixe 198.18.7.0/24 est annoncé par l'AS64496. L'organisation pourrait déléguer l'utilisation de ce préfixe à un client ou

3. En anglais, *hijack*.
4. Internet Routing Registry.
5. Regional Internet Registry.
6. RIPE Network Coordination Centre.

à un partenaire. Dans ce cas, l'attribut `origin` porterait sur un numéro d'AS différent de 64496. Afin d'autoriser certains types de déploiements, il est légitime de déclarer différents objets `route` avec des attributs `route` identiques mais des attributs `origin` différents. L'attribut `mnt-by` indique, quant à lui, les personnes en charge de la déclaration et de la maintenance de cet objet `route`.

Les objets `route` permettent notamment à un fournisseur de transit de filtrer les annonces de ses clients. Ces filtres lui permettent, par exemple, de se prémunir d'erreurs de configuration entraînant des annonces de préfixes ne leur appartenant pas.

1.1.3 La RPKI

Une version sécurisée de BGP, appelée BGPsec[7] [7], est en cours de conception à l'IETF[8]. Dans ce modèle, chaque AS possède un certificat associant une clé publique à un numéro d'AS. Lors de l'annonce d'un préfixe, le routeur inclut une signature comprenant le préfixe, son numéro d'AS et celui de son voisin. Chacun des AS propageant l'annonce ajoute une signature similaire au message BGP. L'intégrité du chemin d'AS peut donc être vérifiée.

La RPKI[9] [8] constitue une étape préliminaire à la mise en œuvre de BGPsec, et introduit notamment un mécanisme permettant de vérifier l'origine d'une annonce. Chaque RIR administre une IGC[10] dédiée à la certification des ressources IP (préfixes IP ou numéro d'AS) dont il a la gestion. Par exemple, le RIPE-NCC est à la racine de la chaîne de confiance dont dépendent les opérateurs européens, et peut délivrer un certificat à chacun d'eux.

Les RIR maintiennent des dépôts contenant les objets de la RPKI signés cryptographiquement. Parmi ces objets, les ROA[11] sont assimilables à des objets `route` plus riches. Ils permettent en effet d'indiquer la longueur maximale des préfixes annoncés par un AS. Par exemple, un `ROA` peut spécifier que l'AS64500 est en droit d'annoncer des préfixes allant de `198.18.0.0/15` à `198.18.0.0/17`. Contrairement aux objets `route`, les ROA peuvent expirer, une période de validité leur étant associée.

1.1.4 Données et outils

L'observatoire utilise les données BGP archivées par le projet RIS [9]. Treize routeurs spécifiques, appelés collecteurs, enregistrent en temps réel l'ensemble des messages BGP qu'ils reçoivent de leurs pairs. La répartition géographique de ces collecteurs permet ainsi d'obtenir la vision locale de l'Internet de plusieurs centaines d'AS.

7. Border Gateway Protocol Security.
8. Internet Engineering Task Force.
9. Resource Public Key Infrastructure.
10. Infrastructure de Gestion de Clés.
11. Route Origin Authorization.

Dans le premier rapport, l'observatoire utilisait uniquement le collecteur de Londres pour calculer les indicateurs BGP concernant les quelques 1500 AS français. Depuis, l'évolution des outils et la mise en œuvre d'une grappe de serveurs a permis d'étendre le périmètre initial.

Les données de tous les collecteurs sont désormais prises en compte pour l'ensemble des 50 000 AS de l'Internet. Pour cela, l'équipe de l'observatoire a adopté différentes techniques [3, 10] de calcul massivement distribué adaptées au traitement des 500 gigaoctets d'archives BGP annuelles.

L'étude de la connectivité des AS français est réalisée à l'aide de l'outil *asrank* [11]. Adapté de travaux académiques [12], il détermine les relations entre AS sous la forme d'un graphe à partir des archives BGP. Les liens entre AS sont alors orientés suivant leur nature (lien de transit ou lien de peering).

Les objets `route` et les `ROA`, utilisés par de nombreux indicateurs BGP, sont accessibles au travers d'interfaces fournies par le RIPE-NCC, notamment via le protocole `whois`. Dans le cadre des usages de l'observatoire, ces interfaces souffrent de différents problèmes comme l'absence d'historique des données et la lenteur des réponses.

Afin de pallier ces problèmes, les données `whois` et RPKI sont téléchargées quotidiennement à partir des dépôts publics des principaux IRR, puis importées dans une base de données. Celle-ci est spécifiquement optimisée pour gérer un grand nombre d'objets, et conçue pour conserver un historique de leurs créations et suppressions. Ainsi, il est possible de calculer les indicateurs pour n'importe quel jour de l'année 2014.

La multiplication des attaques mettant en œuvre BGP et le raccourcissement de leur durée ont conduit l'observatoire à effectuer une partie des traitements, réalisés habituellement hors ligne, en temps réel. Cela permet notamment de lancer, au moyen de sondes Atlas [13], des mesures actives sur l'Internet au cours des incidents.

1.1.5 Évolution des AS français

En 2014, à l'aide de la méthode définie dans les précédents rapports, l'observatoire a identifié 1520 AS français, dont 925 sont visibles dans les archives BGP. La figure 1.3 illustre l'augmentation des AS visibles au cours de l'année. Elle met en évidence quelques variations soudaines en mars, octobre et novembre. Il s'agit d'annonces de préfixes effectuées par des AS de l'enseignement supérieur qui ne sont, la plupart du temps, pas visibles dans l'Internet.

Un noyau dur de 789 AS actifs annonce au moins un préfixe par jour tout au long de l'année 2014, ce qui représente environ 85 % du nombre total d'AS distincts visibles au cours de l'année. Parmi les 15 % d'AS visibles restant, une vingtaine ont été vus pendant moins de 10 jours dans l'année, mais un peu plus de 40 % d'entre eux ont été visibles plus de la moitié de l'année.

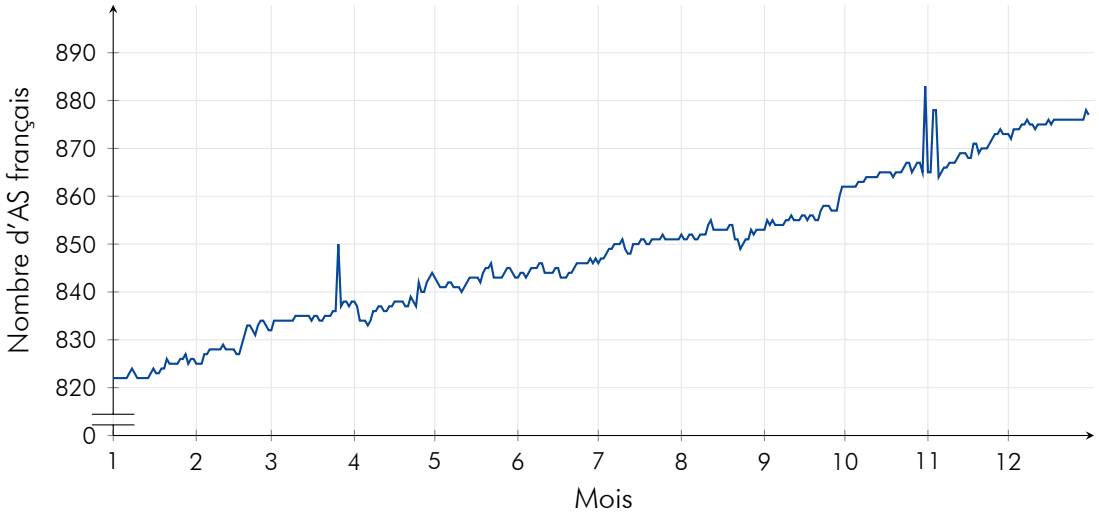


Figure 1.3 – Nombre d'AS français vus dans les archives BGP en 2014

À retenir

En 2014, l'observatoire a identifié 1520 AS français. Parmi ceux-ci, le nombre d'AS actifs, c'est-à-dire ayant annoncé au moins un préfixe, est d'environ 880 fin décembre 2014, contre 850 fin décembre 2013.

1.2 Connectivité des AS français

Afin d'évaluer la robustesse de l'Internet en France, l'observatoire modélise les relations entre AS sous forme de graphes. Ainsi, il existe une arête entre deux AS s'ils sont consécutifs dans un `AS_PATH`. Le type de relation commerciale, *transit* ou *peering*, entre deux AS permet d'orienter les arêtes.

À titre d'exemple, une représentation graphique de la connectivité en IPv4 est donnée dans la figure 1.5. Il apparait que les relations de *peering* sont fortement concentrées au centre. Cela vient du fait que ce type de relation n'est observable que si un des collecteurs est connecté à un des membres de la relation de *peering* ou l'un de ses clients (directs ou indirects).

L'étude des graphes permet également de mettre en évidence les « AS pivots ». Il s'agit d'AS dont la disparition pourrait entraîner la perte de connectivité à l'Internet pour des AS français. Ils apparaissent en vert et orange sur la figure 1.5.

Évolution de l'Internet français

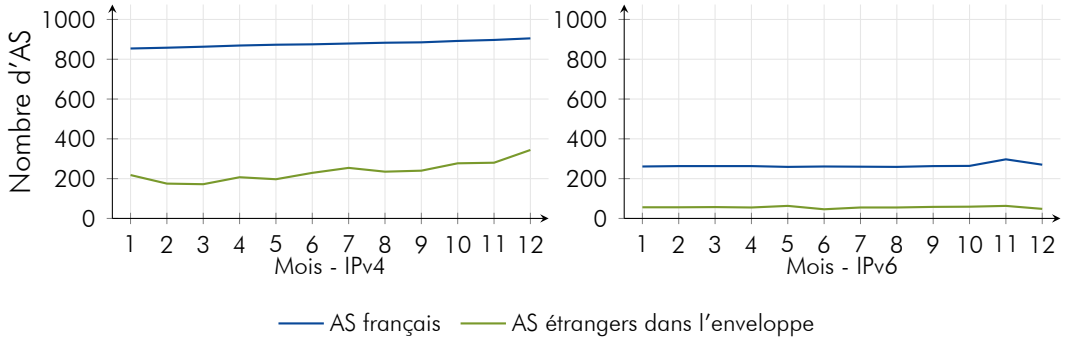


Figure 1.4 – Évolution du nombre d'AS français et de l'enveloppe en 2014

Le graphe ainsi construit permet d'étudier la dynamique de l'Internet au cours de l'année 2014. Le nombre d'AS présents sur des chemins d'AS a ainsi crû de manière linéaire, comme le montre la figure 1.4. En IPv4, le rythme de croissance d'environ 6 % est équivalent à celui observé en 2013. Concernant IPv6, le taux de croissance est équivalent à celui d'IPv4, alors qu'en 2013, il était de 44 %.

L'Internet français est dépendant d'AS étrangers. Certains sont, en effet, nécessaires pour faire transiter le trafic entre AS français. L'enveloppe de l'Internet français contient l'ensemble des AS français et tous les AS se trouvant entre deux AS français sur un `AS_PATH`. Leur nombre est également représenté sur la figure 1.4. En IPv4, ce nombre a crû tout au long de l'année pour atteindre 344. Il est resté stable en IPv6. Comme en 2013, environ 50 AS étrangers sont ainsi nécessaires pour interconnecter tous les AS français en IPv6.

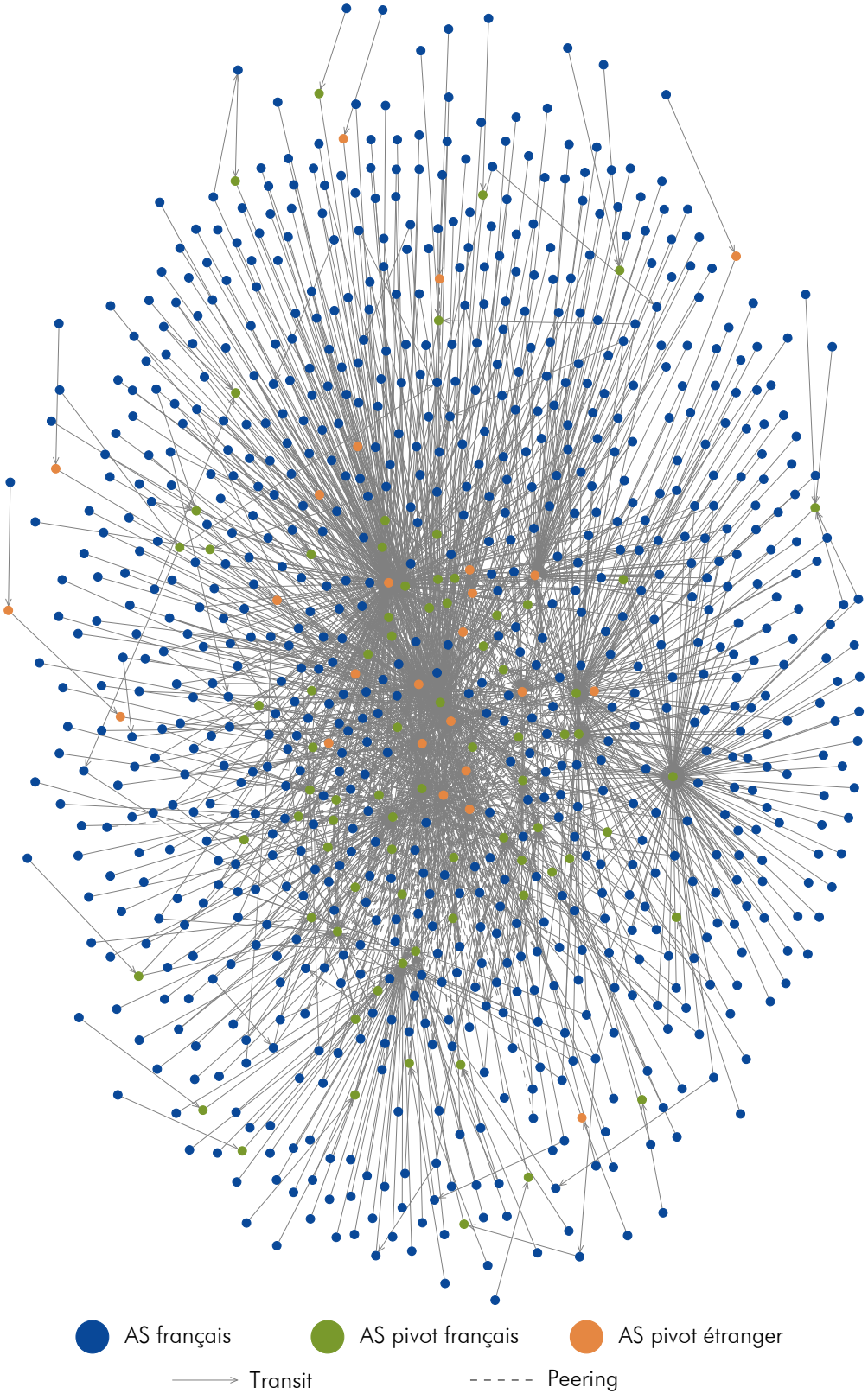


Figure 1.5 – Graphe de connectivité en IPv4 (décembre 2014)

Impacts de la disparition d'un AS

En 2014, le nombre des AS pivots français en IPv4 a nettement augmenté comme le montre la figure 1.6. À l'inverse, le nombre d'AS pivots étrangers est resté stable. En ce qui concerne IPv6, la tendance est différente, et l'on peut noter une diminution du nombre d'AS pivots français et étrangers. C'est une tendance inverse à celle de 2013 qui avait vu le nombre d'AS pivots augmenter de 83 % pour IPv6.

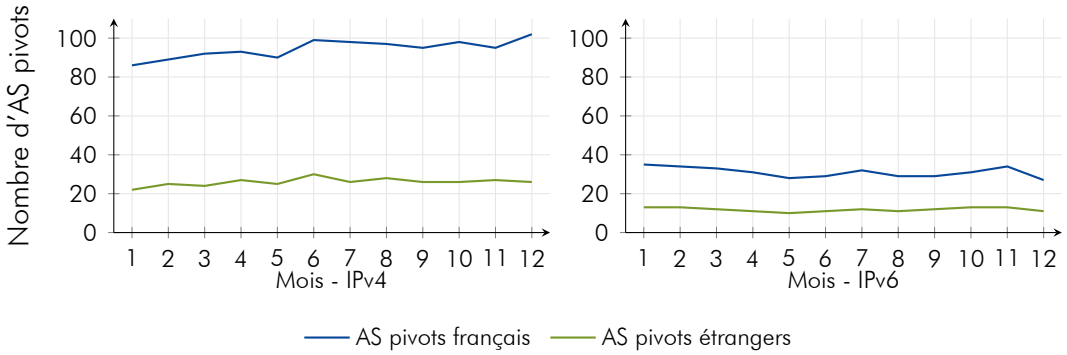


Figure 1.6 – Évolution du nombre d'AS pivots français et étrangers en 2014

Outre le nombre d'AS pivots, l'impact de leurs disparitions est un autre facteur à envisager lors de l'évaluation de la robustesse de la connectivité. Ainsi, la figure 1.7 montre qu'en IPv4, seuls 9 AS pivots affecteraient au moins 10 AS en cas de défaillance. Seuls 24 auraient un impact sur au moins 3 AS. Par conséquent, il existe relativement peu d'AS dont la disparition aurait un impact significatif. En revanche, l'AS pivot le plus critique aurait un impact sur 35 AS, soit 4 % des AS français actifs au même moment. Ces résultats sont en tous points équivalents à ceux de 2013.

À retenir

Concernant l'Internet français, il existe peu d'AS dont la disparition aurait un impact significatif. En 2014, l'impact de la disparition des AS pivots a diminué.

Pour IPv6, la figure 1.8 montre qu'il existe seulement 4 AS pivots pouvant déconnecter au moins 10 AS. Chacun d'entre eux peut cependant affecter entre 10 et 15 AS. De même, 10 AS pivots peuvent avoir un impact sur plus de 3 AS français. En proportion, c'est 37 % des AS pivots contre 23 % pour IPv4.

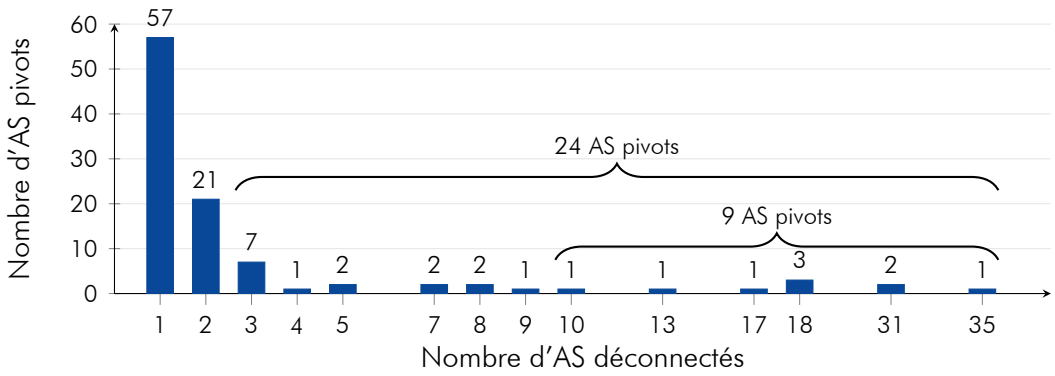


Figure 1.7 – AS pivots en fonction du nombre d'AS déconnectés (IPv4, déc 2014)

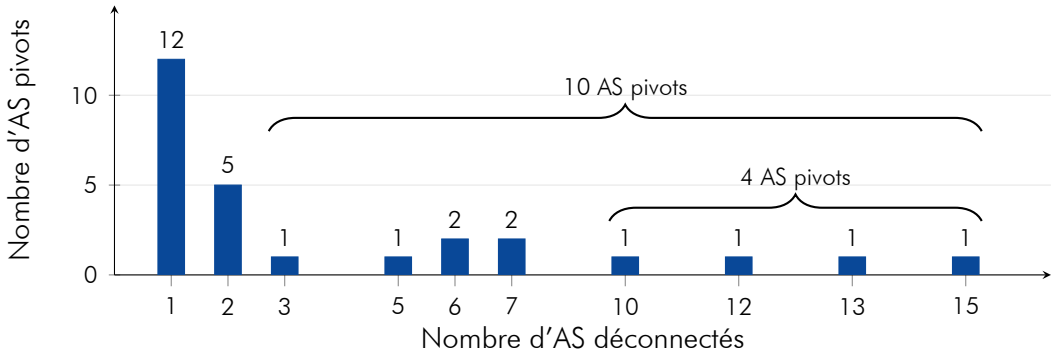


Figure 1.8 – AS pivots en fonction du nombre d'AS déconnectés (IPv6, déc 2014)

À retenir

En 2014, et contrairement à 2013, le nombre d'AS IPv6 a faiblement augmenté, et le nombre d'AS IPv6 pivots a diminué. Cela semble indiquer une augmentation de la densité des interconnexions IPv6.

1.3 Usurpations de préfixes

Les résultats globaux

Au cours de l'année 2014, l'observatoire a détecté 5136 conflits d'annonces. Ils ciblent 283 AS français distincts, et 877 préfixes. La figure 1.9, qui permet d'identifier les différents types de conflits, montre que 79 % d'entre eux ne sont pas des usurpations.

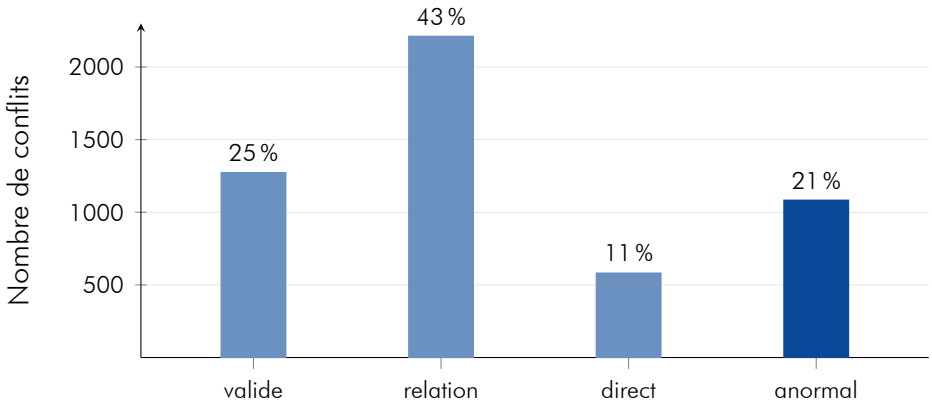


Figure 1.9 – Types de conflits détectés en 2014

Ainsi, les résultats indiquent que 25 % des conflits sont validés par des objets `route` ou des `ROA`. Il s'agit donc d'annonces légitimes pour lesquelles des déclarations ont été effectuées par les gestionnaires des préfixes. Malgré le faible déploiement de la RPKI, une analyse complémentaire a montré qu'environ 1 % des conflits valides sont uniquement vérifiés par des `ROA`.

Les catégories « relation » et « direct » représentent la majorité des conflits. La première identifie des AS dépendants d'une même organisation. La seconde détermine si l'un des deux AS en conflit est fournisseur du second. Par conséquent, ces deux catégories mettent en évidence que 54 % des conflits sont en fait des défauts de déclaration d'objets `route` ou de `ROA`.

Dans une première approche, cette classification en quatre catégories est donc efficace. Ainsi, seuls les 1095 conflits anormaux seront considérés lors de l'identification des usurpations.

Identification en temps réel

Jusqu'à présent, les analyses étaient uniquement effectuées hors ligne, et bien après la survenue des événements. Il était donc impossible de déterminer si le trafic légitime avait pu être redirigé vers l'AS usurpateur [14]. Au cours de l'été 2014, l'observatoire a donc mis en place un traitement des annonces BGP en temps réel. Ce système permet

à la fois de détecter les conflits au plus tôt, et d'effectuer des mesures actives pour identifier des redirections de trafic.

L'analyse temps réel est identique à celle faite hors ligne. Les archives BGP sont cependant téléchargées, puis traitées dès qu'elles sont disponibles. Lorsqu'un conflit anormal est détecté, une mesure active de type `traceroute` est effectuée vers une adresse IP appartenant au préfixe en conflit.

Une mesure `traceroute` identifie le chemin emprunté par les paquets sous la forme d'une liste des adresses IP des routeurs traversés. Cela permet donc de détecter une éventuelle redirection vers l'AS usurpateur.

Il est nécessaire de transformer cette liste d'adresses IP en liste d'AS pour la comparer avec l'`AS_PATH` vu dans les annonces BGP en conflit. Cette opération est difficile car il est délicat d'attribuer un numéro d'AS à des adresses privées, ou à des adresses qui ne sont pas visibles dans les tables de routage BGP. L'observatoire cherche ici à comparer les informations issues du plan de transfert (i.e. les mesures `traceroute`) avec celles du plan de contrôle (i.e. les archives BGP).

Les mesures `traceroute` sont réalisées grâce au projet Atlas [13] du RIPE-NCC qui compte environ 8000 sondes réparties dans près de 4000 AS. En pratique, il existe toujours une sonde appartenant à l'un des AS contenu dans l'`AS_PATH` des annonces conflictuelles.

À retenir

Les mesures actives permettent d'identifier des conflits qui s'accompagnent effectivement d'une redirection de trafic. Elles aident également l'analyse manuelle des usurpations en identifiant des relations entre AS qui ne sont pas visibles dans les archives BGP.

Entre septembre et décembre 2014, près de 300 mesures actives ont été effectuées. Sur les 187 conflits d'annonces identifiés en temps réel, seuls 29 ont fait l'objet de mesures actives car certaines sondes Atlas n'ont pas répondu aux demandes. Il est important de souligner qu'il faut compter une dizaine de minutes entre la détection d'un conflit et la réalisation effective de la mesure. Par conséquent, aucune mesure fiable n'a pu être effectuée pour des conflits courts.

Les réannonces de table globale

Les réannonces de table globale apparaissent suite à des erreurs de configuration des routeurs BGP. Elles se caractérisent par un nombre de conflits important à l'origine d'un même AS pendant un bref laps de temps. L'observatoire a mis en évidence que

21 AS distincts ont probablement effectué de telles réannonces au cours de l'année 2014. Seuls 4 d'entre eux ont annoncé des préfixes en conflit avec des opérateurs français.

Parmi ceux-ci, le premier est un opérateur indonésien [15] qui a annoncé près de 10 000 préfixes qui ne lui appartiennent pas le 2 avril 2014 entre 18h et 20h. Une vingtaine d'AS français ont été concernés par cet incident.
Le second est un AS syrien [16] qui a réannoncé plus de 2000 préfixes le 9 décembre 2014. Cet incident a affecté 7 AS français, pendant une heure environ.

Le troisième est un opérateur sénégalais. Les 11 novembre et 15 décembre, cet AS a annoncé près de 130 préfixes appartenant à différents AS à travers le monde. En temps normal, cet AS annonce 70 préfixes environ. Cet événement a touché une dizaine d'AS français.

Le dernier AS est jordanien, identifié également dans le rapport 2013. Il a régulièrement annoncé entre 1000 et 15 000 préfixes différents par jour [12] entre juillet et décembre 2014. En temps normal, il en annonce une vingtaine. Une quinzaine d'AS français a été touchée.

Les réannonces effectuées par l'AS jordanien et l'AS sénégalais n'ont pas été discutées publiquement. Il s'agit donc d'un résultat tout particulièrement intéressant qui confirme la pertinence des analyses de l'observatoire. Sur les 1095 conflits anormaux, environ 250 correspondent à des réannonces de table globale.

Filtrage automatique des conflits anormaux

Depuis 2011, l'observatoire a affiné ses capacités de détection des usurpations de préfixes à l'aide de filtres appliqués automatiquement. En effet, les analyses menées ces dernières années ont montré que la plupart des conflits anormaux ne sont pas des usurpations, ou ne peuvent être totalement identifiés comme tels.

Avant tout, les conflits anormaux portant sur des préfixes réservés [13], ou trop spécifiques sont filtrés car il est difficile d'en déterminer l'origine exacte. Ceux issus de numéros d'AS spéciaux [14] le sont également. Cette étape permet d'écarter près de la moitié des conflits anormaux. Dans la plupart des cas, il s'agit d'un défaut de déclaration d'objets `route` ou de `ROA`.

Il convient également de filtrer les conflits anormaux entre des AS pour lesquels l'observatoire a identifié des conflits entrant dans les trois autres catégories. En effet, s'il existe des conflits validés par des objets `route` pour certains préfixes, il est probable qu'il existe une relation forte entre les deux AS impliqués. Un peu plus de 10 % des

12. Ces réannonces ont uniquement été reçues par un pair du collecteur situé au DE-CIX à Francfort.
13. Comme le préfixe 6to4 `2002::/16`.
14. Il s'agit des AS privés, de documentations, et de l'AS_TRANS.

conflits anormaux peuvent ainsi être filtrés.

Les usurpations ayant habituellement des durées courtes, la durée des conflits anormaux est ensuite prise en compte afin d'éliminer ceux dont la durée dépasse trois mois. Les conflits issus d'AS français, ou durant moins de dix secondes sont également filtrés. Ces filtres automatiques sont très efficaces et permettent de limiter les analyses à 159 conflits anormaux, au lieu des 1095 initiaux.

Analyse manuelle

Malgré l'efficacité du filtrage automatique, l'équipe de l'observatoire doit étudier manuellement chacun des conflits anormaux restants. Cette étape fastidieuse a nécessité environ une journée de travail.

Environ 70 conflits anormaux correspondent à des erreurs de configuration. Il s'agit principalement de fautes de frappe dans les préfixes ou les numéros d'AS, ou de préfixes relevant d'accord de *peerings* et qui ne devraient pas être annoncés sur Internet. Dans certains cas, il s'agit d'erreurs de fournisseurs de services qui annoncent des préfixes incorrects, ou de reventes de préfixes entre opérateurs. Des opérateurs membres de l'observatoire ont confirmé ce type de comportement.

Cette analyse manuelle a également mis en évidence une trentaine de conflits dont les AS impliqués sont liés. Ce type de relation, très difficile à détecter automatiquement, correspond par exemple à des AS appartenant à des filiales d'un même opérateur international, ou à des accords commerciaux entre opérateurs de transit et clients.

À retenir

Pour l'année 2014, la méthodologie de l'observatoire a isolé une cinquantaine de conflits qui pourraient être des usurpations de préfixes.

Les usurpations de préfixes

Une usurpation de préfixe possède habituellement des caractéristiques bien particulières. L'AS malveillant annonce ainsi un préfixe /24 pendant un laps de temps assez court. Son objectif est de récupérer du trafic, tout en limitant les contre-mesures que peut mettre en place l'AS usurpé.

De février à mai 2014, une vingtaine de conflits correspond à des usurpations utilisées pour voler des *bitcoins* [17] contre plusieurs hébergeurs, dont un français. Ces conflits ont duré entre 5 et 10 heures et ont été effectués par 3 AS différents au Canada et aux

États-Unis.

Entre juillet et novembre 2014, une série de quinze conflits est liée à des campagnes de *spam* [18] menées par un AS russe. Son mode opératoire est un peu particulier car il n'est pas à l'origine des conflits. Il utilise des numéros d'AS inactifs sur Internet afin d'effectuer des usurpations durant une à quatre heures, tout en bénéficiant de nouvelles plages d'adresses IP pour envoyer des courriers électroniques non sollicités.

D'après les données BGP, un AS roumain est à l'origine de ces conflits. Les mesures actives livrent quant à elles une information supplémentaire : le trafic passe bien par l'AS russe. Ce résultat, particulièrement encourageant, montre qu'au-delà de la détection d'usurpations, il est également possible d'identifier des redirections de trafic malveillantes.

À retenir

L'observatoire a identifié qu'une usurpation de préfixes a été utilisée afin de détourner du trafic. L'AS russe incriminé est bien connu pour ses activités d'envoi massif de courriers électroniques non sollicités.

Tout au long de l'année, un important hébergeur français, a par ailleurs, été victime de multiples usurpations qu'il a rapportées publiquement. Les AS usurpateurs sont de pays différents : Colombie, États-Unis et Autriche. Les objectifs de ces usurpations ne sont pas clairs. L'hébergeur français a détecté ces attaques et annoncé des préfixes plus spécifiques pour récupérer son trafic.

En dehors de ces événements rapportés publiquement, sept conflits anormaux demeurent. Leurs caractéristiques semblent indiquer que cinq d'entre eux sont probablement des usurpations de préfixes.

À retenir

L'année 2014 a vu l'émergence de multiples usurpations malveillantes ayant touché des opérateurs français.

1.4 Utilisation des objets route

Les bonnes pratiques soulignent qu'un objet `route` doit être déclaré par un AS pour chaque préfixe qu'il annonce sur Internet. L'indicateur porte sur les deux ensembles illustrés par la figure 1.10 : en bleu, les objets `route` déclarés et en rouge, les préfixes annoncés en BGP. Leur comparaison permet de mettre en évidence les trois sous-indicateurs suivants :

1. les objets `route` pour lesquels aucun préfixe n'est annoncé ;
2. les préfixes ayant au moins un objet `route` associé ;
3. les préfixes couvert par aucun objet `route`.

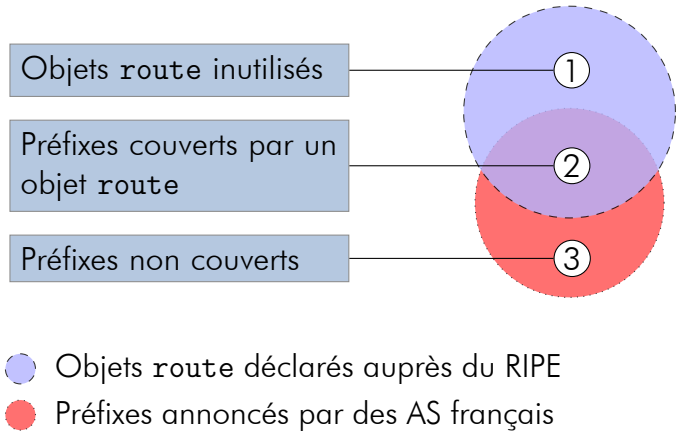


Figure 1.10 – Représentation des sous-indicateurs de l'utilisation des objets `route`

Objets route inutilisés

Les objets `route` déclarés doivent correspondre aux préfixes annoncés par un AS. L'analyse porte ici sur le reliquat d'objets `route` orphelins, c'est-à-dire pour lesquels aucun préfixe n'est annoncé au cours de l'année.

	Type	1er janvier	31 décembre
IPv4	objet `route`	1198	1493
IPv6	objet `route6`	138	180

Table 1.1 – Évolution des objets `route` et objets `route6` inutilisés en 2014

Les objets `route` et objets `route6` inutilisés, présentés dans le tableau 1.1, ont augmenté respectivement de près de 25 % et 30 % au cours de l'année 2014. Cette croissance s'explique par le fait que les destructions d'objet `route` ou objet `route6` sont marginales.

À retenir

Les destructions d'objets `route` et objets `route6` inutilisés ne sont pas systématiques et restent très marginales par rapport aux nouvelles déclarations.

	Type	1er janvier	31 décembre
IPv4	aucun objet `route` déclaré	638	591
	aucun objet `route` utilisé	91	79
IPv6	aucun objet `route6` déclaré	1235	1187
	aucun objet `route6` utilisé	76	106

Table 1.2 – Répartition des AS selon l'usage des objets `route` en 2014

Afin d'analyser les AS du point de vue des objets `route`, l'observatoire les classe dans deux catégories, représentés par le tableau 1.2 :

1. AS n'ayant aucun objet `route` déclaré ;
2. AS n'utilisant aucun objet `route` déclaré.

Pour IPv4, le constat est encourageant, car le nombre d'AS n'ayant aucun objet `route` déclaré diminue, passant de 638 à 591 au cours de l'année. Pour les AS n'utilisant aucun objet `route`, 12 AS qui entraient dans cette catégorie en début d'année ont annoncé progressivement les préfixes correspondants. En effet, ces AS avaient déclaré préventivement les objets `route` auprès du RIPE en 2013, pour annoncer les préfixes correspondant en 2014.

Pour IPv6, la situation pour les AS n'ayant aucun objet `route6` s'améliore : 48 AS ont quitté cette catégorie, montrant que les opérateurs appliquent significativement les bonnes pratiques. En revanche, le nombre d'AS n'utilisant aucun objet `route6` par le biais d'une annonce de préfixe augmente, passant de 76 à 106. Toutefois, il pourrait s'agir ici de déclarations préventives. L'analyse des données de l'année 2015 permettra de valider cette théorie.

À retenir

Certains des objets `route` et `route6` pourraient être des déclarations préventives.

Préfixes couverts par des objets route

Préfixes	1er janvier	31 décembre
IPv4	4146	4219
IPv6	315	361

Table 1.3 – Évolution des préfixes couverts en 2014

Les préfixes IPv4 et IPv6 couverts, représentés par le tableau 1.3, ont crû au cours de l'année. La catégorie de préfixes IPv4 a augmenté de 73 nouveaux préfixes. Les déclarations d'objets `route` en IPv4 continuent de s'améliorer. Pour IPv6, la couverture des préfixes a significativement augmenté passant de 315 à 361 préfixes.

AS	1er janvier	31 décembre
IPv4	686	730
IPv6	199	214

Table 1.4 – Évolution des AS ayant tous leurs préfixes couverts en 2014

Les opérateurs déclarent de plus en plus systématiquement les objets `route` et `route6` pour les préfixes qu'ils annoncent. L'observatoire, se concentre ici sur les AS dont tous les préfixes sont couverts. Les résultats sont présentés dans le tableau 1.4.

Pour IPv4, 44 AS ont rejoint l'ensemble des AS pour lesquels chaque préfixe est couvert par au moins un objet `route`. Pour IPv6, le constat est le même. 15 AS ont vu tous leurs préfixes couverts au cours de l'année, montrant que l'effort de déclaration n'est pas exclusif à IPv4. Il est important de noter que pour ces deux protocoles, l'augmentation est principalement due à de nouveaux opérateurs apparus au cours de l'année.

À retenir

Les analyses, par préfixe et par AS, confirment l'application des bonnes pratiques pour IPv4 et IPv6.

Préfixes non couverts par des objets route

La politique de filtrage des préfixes, appliquée par les opérateurs de transit, vis-à-vis de leurs clients, peut être basée sur les objets `route`. Ce sous-indicateur permet de mettre en évidence ce qui pourrait se passer si tous les opérateurs de transit filtraient strictement les préfixes sur la base des objets `route`. Par conséquent, l'analyse s'intéresse aux préfixes non couverts.

Préfixes	1er janvier	31 décembre
IPv4	1217	839
IPv6	150	121

Table 1.5 – Évolution des préfixes non couverts en 2014

L'analyse du tableau 1.5 montre une nette amélioration pour les préfixes non couverts en 2014. En effet, ces derniers ont diminué de 31 % pour IPv4 et 19 % pour IPv6. Les préfixes concernés ont, fait l'objet de déclarations d'objets `route` ou objets `route6`, ou ont tout simplement arrêté d'être annoncés.

Préfixes	1er janvier	31 décembre
IPv4	162	170
IPv6	59	51

Table 1.6 – Évolution des AS avec au moins un préfixe non couvert en 2014

Pour les AS, l'observatoire considère les catégories formées par les AS dont au moins un préfixe n'est pas couvert un objet `route` ou `route6`, et sont représentées par le tableau 1.6. L'ensemble des AS, en IPv4, évolue très peu au cours de l'année. Seuls 8 nouveaux AS y ont fait leur apparition. Cet ensemble est constitué d'un noyau dur d'AS ne déclarant aucun objet `route`, ou ne mettant pas à jour ces derniers au même rythme que les annonces de nouveaux préfixes.

Pour IPv6, 8 AS parmi les 59 en début d'année, ont appliqué les bonnes pratiques en déclarant systématiquement les objets `route6` pour chacun de leurs préfixes.

À retenir

En 2014, les opérateurs déclarent plus systématiquement les objets `route6`, améliorant la situation constatée en 2013.

1.5 Déclarations dans la RPKI

Évolution de la couverture de l'espace d'adressage

L'étude des déclarations effectuées dans le dépôt du RIPE-NCC de la RPKI montre une forte croissance du nombre d'AS participants au cours de l'année 2014. Au début du mois de janvier, 111 AS français avaient des ROA dans la RPKI. Au 31 décembre, la RPKI contient des déclarations issues de 199 AS français, ce qui représente une augmentation de près de 80 %.

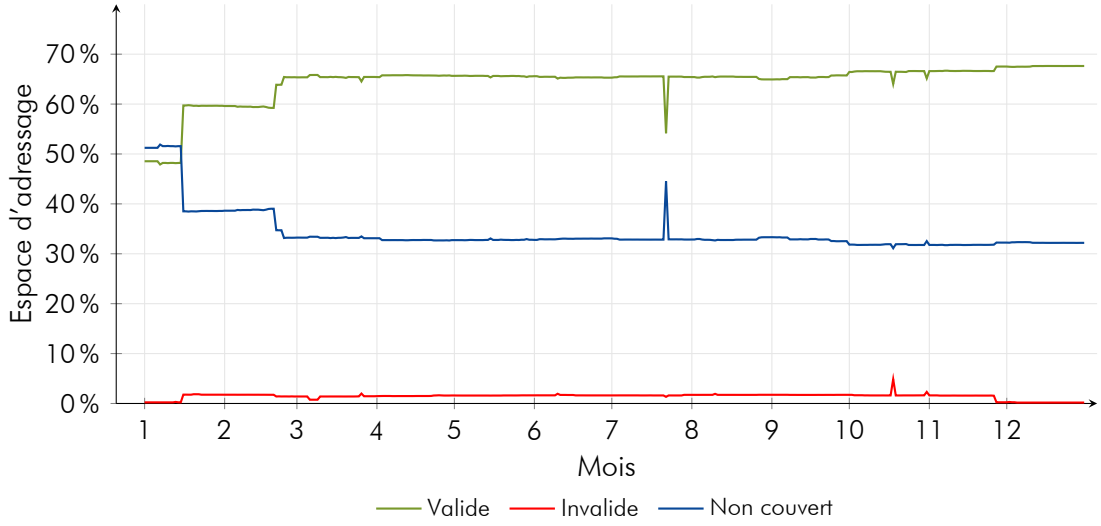


Figure 1.11 – Couverture de l'espace d'adressage IPv4 par la RPKI en 2014

Afin de caractériser les conséquences de cette augmentation, l'évolution de la couverture de l'espace d'adressage IPv4 géré par les AS français au cours de l'année 2014 est donnée par la figure 1.11. Outre quelques variations ponctuelles et brusques principalement dues à des annonces de routes erronées, elle traduit une augmentation significative du pourcentage de l'espace d'adressage valide au cours de l'année. Ainsi, au 31 décembre 2014, un peu plus de 67 % de l'espace d'adressage est valide selon la RPKI, contre environ 48 % au début de l'année 2014.

Le pourcentage de l'espace d'adressage non couvert et de l'espace d'adressage invalide ont en conséquence tous deux baissé au cours de l'année. Au 31 décembre 2014, 32 % de l'espace d'adressage n'est pas couvert. Le pourcentage de l'espace d'adressage invalide reste, quant à lui, relativement faible au cours de l'année. À la fin de l'année 2014, ce pourcentage est de moins de 0,2 %.

En ce qui concerne IPv6, l'espace d'adressage géré par les AS français est très faiblement couvert par les déclarations de la RPKI. À la fin de l'année 2014, les ROA couvrent moins de 1 % de cet espace d'adressage.

Validité des annonces effectuées par les AS français

Afin d'avoir un aperçu de l'impact potentiel sur la connectivité d'un filtrage strict basé sur les données de la RPKI, l'étude s'est également portée sur le nombre d'AS effectuant uniquement des annonces valides ou invalides.

Le nombre d'AS effectuant uniquement des annonces de préfixe valides augmente au cours de l'année 2014. De 51 en janvier 2014, ce nombre passe à 100 à la fin de l'année. Par ailleurs, le nombre d'AS effectuant uniquement des annonces de préfixes invalides, bien qu'ayant connu des augmentations ponctuelles au cours de l'année, a décru pour passer de 6 en janvier 2014 à 3 en décembre 2014.

Ces résultats montrent qu'en cas de filtrage strict basé sur la RPKI, seuls 11 % des AS actifs à la fin de l'année 2014 verraient l'ensemble de leurs routes propagées dans l'Internet. Par ailleurs, l'espace d'adressage géré par 3 AS ne serait plus joignable.

Utilisation potentielle de la RPKI par les AS français

Les analyses effectuées sur les données du dépôt du RIPE-NCC ne permettent pas de mesurer l'utilisation réelle, par les AS français, de la RPKI. Cependant, cette analyse montre une augmentation significative d'un usage potentiel de la RPKI par les AS français. Malgré cette progression, la couverture de l'espace d'adressage géré par ces derniers n'est pas suffisante pour pouvoir envisager un filtrage strict basé sur les `ROA`.

À retenir

L'année 2014 a connu une forte augmentation du nombre d'AS français ayant publié au minimum un `ROA` dans la RPKI. Cependant, les déclarations effectuées dans la RPKI sont loin d'être exhaustives : à la fin de l'année 2014, près d'un tiers de l'espace d'adressage IPv4 n'est pas couvert. Pour le protocole IPv6, la couverture est très faible : plus de 99 % de l'espace d'adressage n'est pas couvert par les `ROA`.

Chapitre 2

Résilience sous l'angle du protocole DNS

2.1 Introduction

Le système de noms de domaine, géré par le protocole DNS [19, 20], est un système de nommage réparti et hiérarchique dont les deux objectifs essentiels sont d'associer à une adresse IP un nom lisible par les utilisateurs. Ainsi, l'adresse IP `2001:67c:2218:2::4:20` correspond au nom de domaine `www.afnic.fr`. Dans le cas d'un changement d'hébergeur, seul le responsable du domaine doit modifier l'adresse IP pointée par le nom. Grâce au DNS, ce changement est donc transparent pour les utilisateurs.

La structure du DNS est illustrée dans la figure 2.1. Au sommet de la hiérarchie se trouve la racine représentée par un point « . ». Il s'agit du point final que l'on retrouve au niveau des noms de domaine comme « `www.afnic.fr.` ».

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. Ce rapport ne tient pas compte de la différence subtile entre domaine et zone. Par conséquent, ces deux termes y sont employés indifféremment.

Une zone peut être « déléguée » afin de confier la gestion de ses données à un organisme différent de celui qui administre la zone déléguante, appelée alors zone parente.

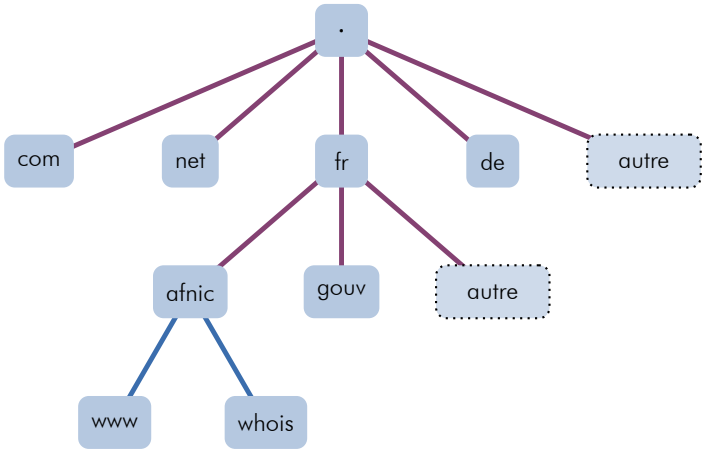


Figure 2.1 – Structure du DNS

À titre d'exemple, la zone `.fr` a été déléguée à l'Afnic qui fixe les règles d'attribution des noms de domaine sous `.fr`, indépendamment de sa zone parente, la racine, gérée par l'ICANN [1]. Les délégations sont illustrées par des liens violets dans la figure 2.1.

Les informations stockées dans le DNS

Les ressources attachées à une zone sont décrites par des enregistrements DNS. Chaque enregistrement DNS comporte un nom de domaine qui se décline à partir de celui de la zone (exemple : le nom `www.afnic.fr` sous la zone `afnic.fr`), un type (exemple : `AAAA`, pour désigner une adresse IPv6) et des données qui dépendent du type en question.

Les différents types d'enregistrement DNS sont publiés et maintenus par l'IANA [2] dans un registre dédié aux paramètres du DNS [21]. À titre d'exemples, les types d'enregistrement suivants sont étudiés dans ce rapport :

- `A` : une adresse IPv4 ;
- `AAAA` : une adresse IPv6 ;
- `MX` : le nom d'un relais de messagerie électronique entrants ;
- `NS` : le nom d'un serveur DNS.

Interroger le DNS

La résolution DNS est le mécanisme qui permet de récupérer les enregistrements associés à un nom de domaine et à un type donnés. Ce mécanisme de résolution fait intervenir deux types de serveurs DNS, comme l'illustre la figure 2.2, qui met en évidence des interactions numérotées :

- **un serveur récursif** (également appelé serveur cache ou résolveur). La machine de l'utilisateur le connaît et lui soumet ses requêtes DNS (interaction 1). Ce serveur, habituellement géré par un FAI [3], va alors interroger l'arborescence DNS en partant de la racine (interaction 2) et en suivant de proche en proche les points de délégation 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 de l'utilisateur (interaction 5) et conserve en mémoire (fonction de cache) les informations reçues ;
- **des serveurs faisant autorité** pour des zones données, qui répondent au serveur récursif. Soit ils font effectivement autorité pour le nom de domaine demandé par la machine utilisateur, et ils lui retournent la réponse ; soit ils l'aiguillent vers d'autres serveurs à interroger qui seraient plus susceptibles de faire autorité pour le nom de domaine recherché.

1. Internet Corporation for Assigned Names and Numbers.
2. Internet Assigned Numbers Authority.
3. Fournisseur d'Accès à Internet.

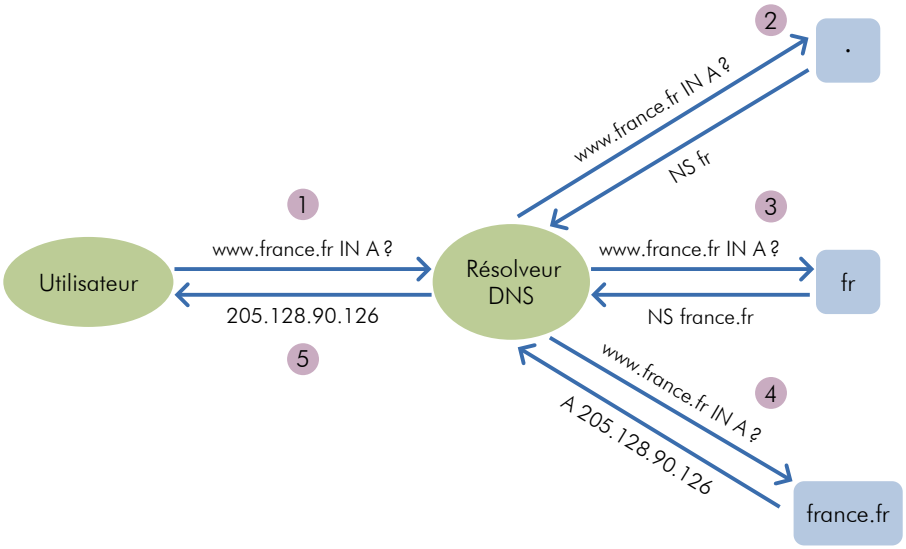


Figure 2.2 – Résolution DNS

La sécurité des enregistrements

Conçu à une époque où la menace était moins forte, le DNS ne bénéficiait pas de mécanismes de sécurité avancés lors à sa création. Le protocole DNSSEC vise à remédier à ce manque [22]. Ce dernier permet d'assurer l'authenticité et l'intégrité des données en s'appuyant sur des mécanismes de cryptographie asymétrique. Les clés publiques et les signatures sont respectivement stockées dans des enregistrements `DNSKEY` et `RRSIG`. La chaîne de confiance DNSSEC [4] est établie et maintenue grâce à des enregistrements `DS`. Ce mécanisme empêche les attaques dites de « pollution de cache » visant à injecter des enregistrements frauduleux dans un serveur récursif.

2.1.1 Données et outils

L'observatoire utilise `DNSwitness` [23], plateforme multi-usage développée par l'Afnic et permettant de réaliser des mesures via le DNS.

`DNSdelve` est l'une des deux composantes de `DNSwitness`. Il permet d'effectuer des mesures actives. Il prend en entrée une liste de zones (toutes les zones déléguées sous `.fr` par exemple), effectue des requêtes DNS sur les zones en question et stocke les résultats en base de données. `DNSdelve` comporte plusieurs modules spécialisés, utilisables de manière indépendante. Pour les besoins de l'observatoire, plusieurs modules sont utilisés pour fournir les résultats des indicateurs de dispersion des serveurs DNS faisant autorité, et de déploiement du protocole IPv6.

`DNSmezzo`, la seconde composante de `DNSwitness`, est un outil de mesures passives. Il se présente sous la forme d'une sonde placée au niveau d'un serveur DNS dont on

4. DNS SECurity extensions.

veut analyser le trafic. DNSmezzo capture et analyse les requêtes reçues par le serveur et sauvegarde les résultats dans une base de données.

Données utilisées

Toutes les mesures actives ont été réalisées en utilisant la zone .fr qui varie au gré des créations, suppressions et modifications de zones déléguées. De 2013 à 2014, le nombre de ces zones déléguées a augmenté de 5,1 % pour atteindre le nombre de 2 853 793 au 31 décembre 2014, contre 2 716 055 au 31 décembre 2013.

En 2014, la zone .fr représentait 36,5 % du marché des noms de domaine en France [24]. Pour cette raison, les résultats obtenus pour chacun des indicateurs DNS ne se prétendent pas représentatifs de tous les noms de domaines enregistrés sur le territoire.

Les mesures actives sont effectuées de manière hebdomadaire pour chacun des modules de DNSdelve. Ce dernier calcule, à chaque lancement, un échantillon aléatoire représentant 10 % de la copie du jour de la zone .fr, soit environ 285 000 zones déléguées pour l'année 2014.

Les chiffres présentés dans ce rapport pour la partie active de la plateforme proviennent des résultats des mesures lancées en décembre 2014. Les données de DNSmezzo proviennent, quant à elles, des cinq sondes, chacune installée au niveau d'une instance de d.nic.fr, serveur *anycasté* [22] et administré par l'Afnic. Ces sondes se situent en région parisienne, à Lyon, Londres, Francfort et Bruxelles. Les données ainsi récoltées sont utilisées pour étudier la progression du protocole IPv6.

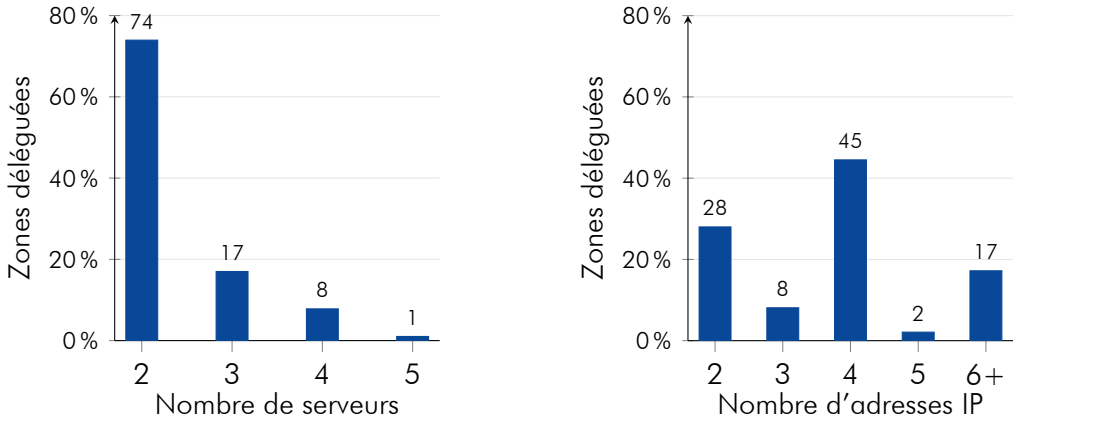
Il faut noter qu'en basant les analyses sur le serveur d.nic.fr uniquement, les résultats sont biaisés en faveur des requêtes DNS en provenance du territoire français. En effet, les instances de d.nic.fr présentes en France reçoivent plus de requêtes en provenance d'opérateurs français que celles qui se trouvent à l'étranger.

En pratique, en tenant compte de l'ensemble des sondes, l'observatoire effectue 16 mesures par semaine : 10 les mardis et jeudis, et 6 les samedis et dimanches. Elles s'effectuent avec un échantillonnage aléatoire de 5 % des requêtes reçues durant 24 heures. Cela représente un volume important car les 8 instances de d.nic.fr reçoivent environ 4000 requêtes par seconde (moyenne en journée et en pleine semaine). Le nombre de requêtes DNS, toutes sondes confondues, est de l'ordre de 130 millions de requêtes par semaine en décembre 2014.

2.2 Dispersion des serveurs DNS faisant autorité

Nombre de serveurs par zone déléguée

Pour ce nouveau rapport, l'observatoire a modifié la méthodologie utilisée. Jusque-là, le nombre d'adresses IP des serveurs DNS faisant autorité pour une zone était comptabilisé. Un serveur DNS pouvant avoir plusieurs adresses IPv4 et IPv6, un biais pouvait être introduit. Cette année, le nombre de d'enregistrements `NS` associés aux zones déléguées sous la zone de `.fr` est utilisé.



(a) Nombre de serveurs par zone déléguée

(b) Nombre d'adresses IP par zone déléguée

Figure 2.3 – Dispersion des zones déléguées en décembre 2014

Le biais de la méthode précédemment utilisée est représenté dans la figure 2.3b. Il ressort que les serveurs DNS ayant à la fois des adresses IPv4 et IPv6 augmentaient la proportion des zones ayant 4 et plus de 6 serveurs. La nouvelle méthodologie illustre ainsi qu'en 2014, près de trois-quarts des zones sont hébergées sur seulement deux serveurs faisant autorité. Ce chiffre, bien que semblant suffisant au regard des bonnes pratiques admises [19], nécessite d'être affiné par l'analyse des autres sous-indicateurs de ce chapitre.

Nombre d'AS par zone déléguée

La dispersion topologique des serveurs DNS est une exigence issue de l'ingénierie de la résilience [25, 26]. En 2014, le nombre moyen d'AS par zone reste équivalent à celui de 2013, et stagne à 1,3. Par ailleurs, la quantité de zones dans un seul AS reste stable depuis 2011, culminant à 82 % des zones déléguées.

La dispersion des serveurs DNS dans des AS différents reste donc toujours faible avec la majeure partie des zones ayant tous leurs serveurs au sein d'un unique AS. Facteur aggravant, les quatre premiers AS en termes d'hébergement de serveurs DNS gèrent à

eux seuls 70 % de ces serveurs.

À retenir

Pratiquement toutes les zones ont au moins deux serveurs DNS, cependant ceux-ci sont généralement localisés dans un seul AS.

Dispersion des serveurs par pays

Plus de 80 % des zones déléguées ont leurs serveurs de noms dans un seul pays. La figure 2.4 pointe les trois pays où se trouve le plus grand nombre de serveurs DNS faisant autorité pour la zone `fr`. Si la France est toujours prééminente avec 59 % des serveurs, sa part diminue néanmoins au profit de l'Allemagne.

De plus, les Pays-Bas qui se plaçaient jusque-là en cinquième position, se retrouvent en 2014 en quatrième position, le cinquième pays étant cette année le Danemark, où se trouve 1,1 % des serveurs.

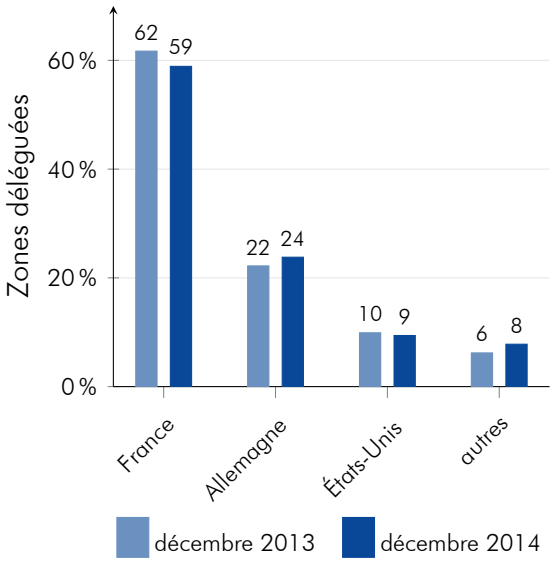


Figure 2.4 – Dispersion des serveurs sur les pays les plus couvrants

2.3 Dispersion des relais de messagerie entrants

2.3.1 Description

Les adresses de courrier électronique sont divisées en deux parties par le symbole `@`. La partie gauche désigne la boite aux lettres du destinataire, tandis que la partie droite est le nom de domaine. Ce nom de domaine est interrogé, grâce au DNS, par les relais de messagerie sortants des expéditeurs de courriers électroniques. Ils y recherchent des enregistrements de type `MX`, qui désignent les relais de messagerie entrants du nom de domaine destinataire. Les relais de messagerie sortants initient ensuite une connexion TCP avec le protocole SMTP vers les relais de messagerie entrants pour délivrer le courrier électronique.

Ce schéma de communication implique donc une dépendance des relais de messagerie au bon fonctionnement du DNS. Ainsi, l'impossibilité de récupérer les enregistrements MX résulte en l'incapacité d'acheminer les courriers électroniques à destination du nom de domaine affecté.

Cet indicateur a pour l'objectif d'offrir un aperçu de la résilience des relais de messagerie entrants du point de vue du DNS. Pour cela, trois mesures sont effectuées :

- **nombre de relais par zones déléguées** : calcul du nombre de relais de messagerie entrants distincts par zones étudiées ;
- **dépendance des relais à des noms de serveur tiers** : étude des noms renseignés dans les enregistrements MX et de leur présence éventuelle hors de la zone considérée ;
- **concentration des relais de messagerie entrants** : détermination du regroupement éventuel des relais sur des plateformes d'hébergement ou de leur répartition uniforme.

2.3.2 Méthodologie de mesure

L'ensemble des enregistrements NS contenus dans la zone `fr` est obtenu par simple extraction de la zone. Ensuite, pour chaque zone déléguée, une requête DNS portant sur les enregistrements MX est envoyée. Des précautions ont été prises afin de limiter la charge des serveurs interrogés lors de la campagne de mesures effectuée fin décembre 2014.

La première étude consiste à compter le nombre d'enregistrements MX par zone. Cela permet de mesurer la capacité des domaines étudiés à résister à une indisponibilité partielle de leurs relais de messagerie entrants.

La relation de dépendance à des noms de serveur tiers constitue la seconde étude. Pour cela, les zones sont classées en fonction du nom de serveur renseigné dans leurs enregistrements MX. Ainsi, lorsque tous les relais sont désignés par des noms de serveur hors de la zone interrogée, cette zone est considérée comme ayant des relais

« dépendants » de noms de serveur tiers. Toutes les autres zones déléguées sont classées comme ayant des relais « indépendants ». Les relais dépendants sont exposés à des risques d'indisponibilité en cas de défaillance de l'ensemble des noms de serveur tiers dont ils dépendent.

Afin d'affiner les données précédentes, l'étiquette [5] correspondante au TLD est extraite des noms de serveur renseignés dans les enregistrements MX. Chaque enregistrement MX est considéré indépendamment de la zone dans laquelle il se trouve. Ainsi, une zone dont les relais de messagerie entrants sont `mx0.example.com` et `mx1.example.net` sera ajoutée à la fois pour le compte de `com` et de `net`.

L'analyse de concentration des relais emploie deux approches complémentaires. La première permet de constater la concentration sur un même nom de serveur. Il suffit, pour cela, de compter le nombre d'occurrences d'un même nom de serveur sur l'ensemble des enregistrements MX. Cette méthode présente cependant un défaut. Elle ne permet pas de dégager des tendances de concentration sur des acteurs. En effet, certains répartissent les relais de messagerie dont ils reçoivent la gestion, sur de nombreux noms de serveur. La seconde approche ne considère que les deux étiquettes du nom de domaine les plus à droite [6]. Ainsi, deux relais désignés par les noms `mx0.example.com` et `mx1.example.com` seront comptabilisés comme étant tous deux en rapport avec `example.com`.

Limitations

Pour cette étude, les noms de serveurs ne sont pas résolus en adresses IP. Certains chiffres sont donc potentiellement pessimistes : ils ne tiennent pas compte du cas où plusieurs adresses IP sont renvoyées pour un même nom de serveur. Dans ce cas, la présence d'un seul enregistrement MX n'équivaut pas nécessairement à un SPOF [7].

2.3.3 Résultats et analyse

Nombre de relais par zone déléguée

Les zones étudiées présentent un faible nombre de relais de messagerie entrants, en moyenne. Ainsi, un seul relais est disponible pour 42 % des zones déléguées, comme l'indique la figure 2.5. En cas d'incident, la défaillance de ce relais unique provoque alors une indisponibilité totale du service.

Du point de vue du DNS, les relais de messagerie entrants auraient donc une résilience moindre que les serveurs DNS. En effet, les zones étudiées possèdent toujours au moins

5. En anglais, *label*.
6. Cette stratégie est possible pour la zone `fr`, qui délègue la plupart des noms de second niveau. Elle ne peut cependant s'appliquer à tous les registres.
7. Single Point Of Failure.

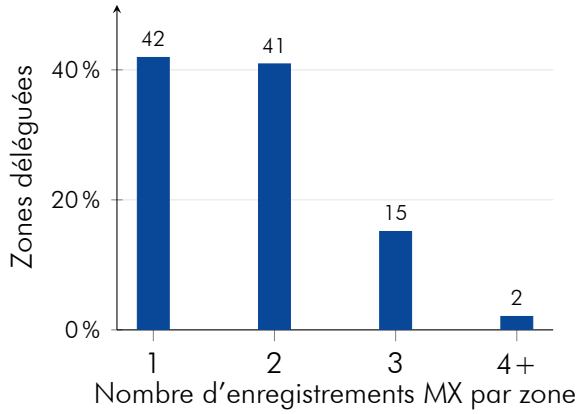


Figure 2.5 – Dispersion des relais de messagerie entrants par domaine en 2014

deux enregistrements NS, comme le montre la figure 2.3a de la page 35. Il importe cependant de noter que le service de messagerie reposant sur SMTP comprend de nombreux mécanismes permettant de pallier des erreurs temporaires. Le risque de perte de courrier électronique s'en retrouve réduit.

À retenir

Un seul relais de messagerie est renseigné pour 42 % des zones déléguées. Le risque d'impossibilité de recevoir de nouveaux messages électroniques est donc accru par la présence d'un SPOF.

Dépendance des relais à la résolution de noms de serveur tiers

Le faible nombre de relais par zone est à considérer également en regard du risque d'échec de résolution des noms de serveur les désignant. En effet, 77 % des domaines étudiés ont des relais dépendants, d'après la figure 2.6. Leur résilience pourrait donc être affectée en cas d'incident lors de la résolution de tous les noms de serveur tiers. Ce risque est d'autant plus marqué qu'en affinant ces données, il apparaît un manque de diversité dans le choix des TLD. En effet, dans 99 % des cas, tous les enregistrements MX pointent vers des noms dans un même TLD.

Il convient de noter qu'un nom de serveur est dépendant, au minimum, des domaines situés au-dessus de lui dans l'arborescence DNS. Ainsi, tous les sous-domaines de `fr` sont nécessairement dépendants de `fr` et de la racine du DNS. En utilisant des noms de serveur situés hors de la zone considérée, de nouvelles dépendances sont ainsi créées. Une dépendance est, par exemple, ajoutée en employant un nom de serveur situé sous

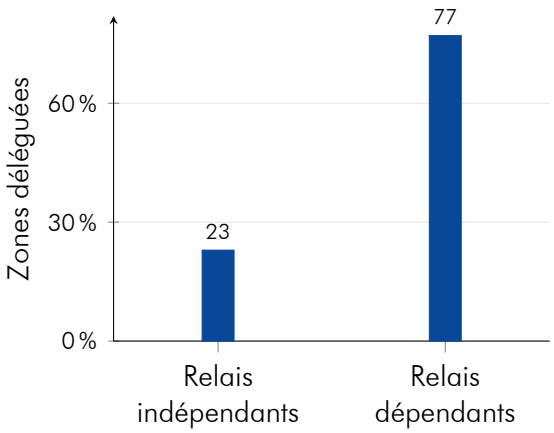


Figure 2.6 – Classement par dépendance des relais à des noms de serveur tiers

le même TLD que la zone considérée. En utilisant un nom de serveur situé sous un autre TLD, au minimum deux dépendances sont ajoutées : celle au nouveau TLD, et celle au nom de domaine situé sous ce TLD et contenant le nom de serveur renseigné dans l'enregistrement MX.

Concernant l'année 2014, l'étude fine des données révèle que 36 % des zones étudiées disposent de seulement un relais de messagerie et que ce dernier est désigné par un nom de serveur situé hors de la zone considérée. Cela signifie donc que 36 % des zones déléguées peuvent subir une perte totale de service par le dysfonctionnement d'un nom de serveur tiers et que la liste des tiers pouvant causer cet impact n'est pas minimale.

À retenir

Près de 77 % des zones déléguées depuis `fr` présentent des relais de messagerie entrants dépendants de noms de serveur tiers. Cette configuration accroît leur risque d'indisponibilité, la liste des tiers dont ils sont dépendants n'étant pas minimale.

Analyse fine par domaines de premier niveau

Les relais dépendants s'avèrent être désignés par des noms de serveur situés sous un autre TLD que `fr` dans 77 % des cas, comme représenté en bleu clair dans la figure 2.7. Ces relais dépendants sont donc encore plus exposés à des risques d'indisponibilité que s'ils avaient été uniquement dépendants d'un nom situé sous `fr`. En effet, la résolution de ces noms requiert le suivi avec succès d'un plus grand nombre de délégations. Par

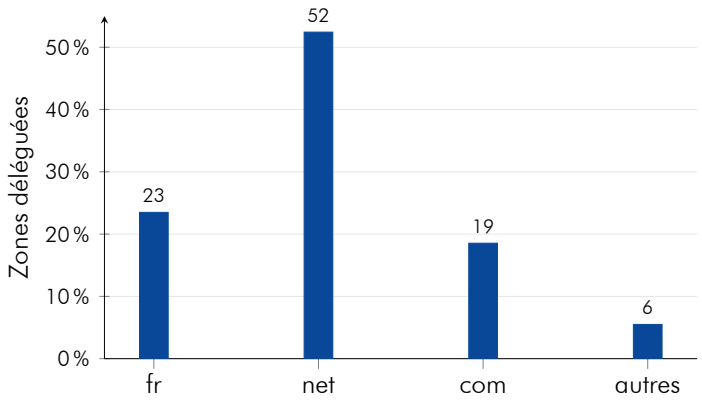


Figure 2.7 – Répartition des zones déléguées avec relais dépendants, par TLD

ailleurs, il importe que 71 % des relais sont dépendants de `com` et `net`, géré par un même opérateur.

Concentration des relais de messagerie entrants

Afin de déterminer la concentration des relais sur des plateformes d'hébergement, la première méthode employée consiste à compter le nombre d'occurrences d'un même nom dans les enregistrements MX.

Il apparaît ainsi une forte concentration sur quelques noms de serveur. En effet, 68 % des enregistrements MX font référence à l'un des dix noms les plus fréquents.

En outre, 14 % des relais des zones étudiées sont dépendants d'un unique et même nom de serveur situé, de surcroît, sous un TLD tiers. Cette concentration sur un unique nom présente un risque non négligeable pour l'intégrité et la disponibilité du service de courrier électronique pour les zones concernées.

La seconde méthode d'analyse des données repose sur l'étude des noms de second niveau. Elle révèle une concentration forte sur quelques acteurs. Ainsi, la moitié des relais de messagerie entrants sont désignés par des noms de serveur correspondant à deux plateformes d'hébergement, comme l'indique la figure 2.8. L'indisponibilité de l'un de ces acteurs influencerait significativement la disponibilité d'une fraction notable des relais de messagerie entrants français.

Il importe néanmoins de noter que la concentration des relais de messagerie entrants ne reflète pas le nombre d'utilisateurs. Dans ces résultats, un relais de messagerie d'une petite entreprise a donc le même poids que le relais d'un fournisseur d'accès à l'Internet.

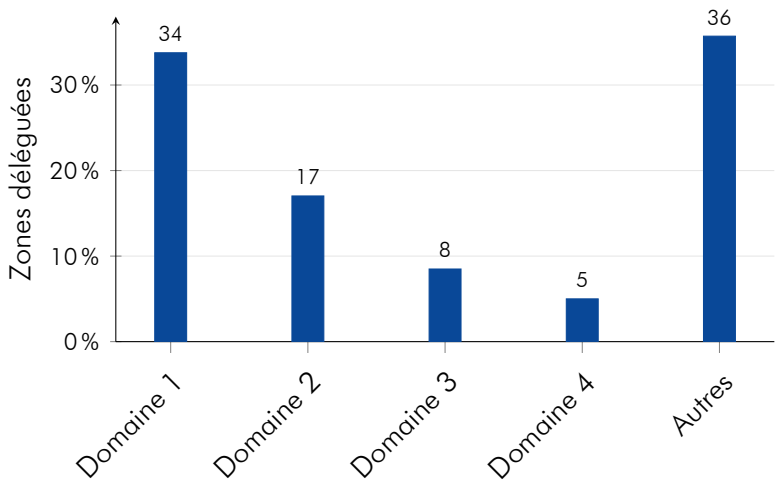


Figure 2.8 – Concentration des relais par noms de second niveau en 2014

À retenir

Les relais de messagerie entrants sont fortement concentrés sur un faible nombre de plateformes d'hébergement. Deux acteurs couvrent à eux seuls 51 % des relais de messagerie étudiés. Leur indisponibilité causerait un impact significatif sur les zones considérées.

2.4 Taux de pénétration de DNSSEC

La figure 2.9 indique la progression du nombre de zones signées au cours des dernières années. À partir de 2014, il s'agit du nombre d'enregistrements DS [8] extraits de la zone `.fr`. Avant, il était calculé avec `DNSdelve` sur un échantillon de 10 % de la zone.

Proportionnellement à la taille de la zone `.fr`, le taux de zones possédant un DS dans la zone parente reste assez faible : il représentait 1,5 % des zones en 2012, 3,8 % en 2013 et 7 % en 2014.

En décembre 2013, environ 91 000 zones déléguées possédaient un enregistrement DS dans la zone `.fr` contre 197 000 en décembre 2014. Cette évolution correspond à une hausse de 116 %.

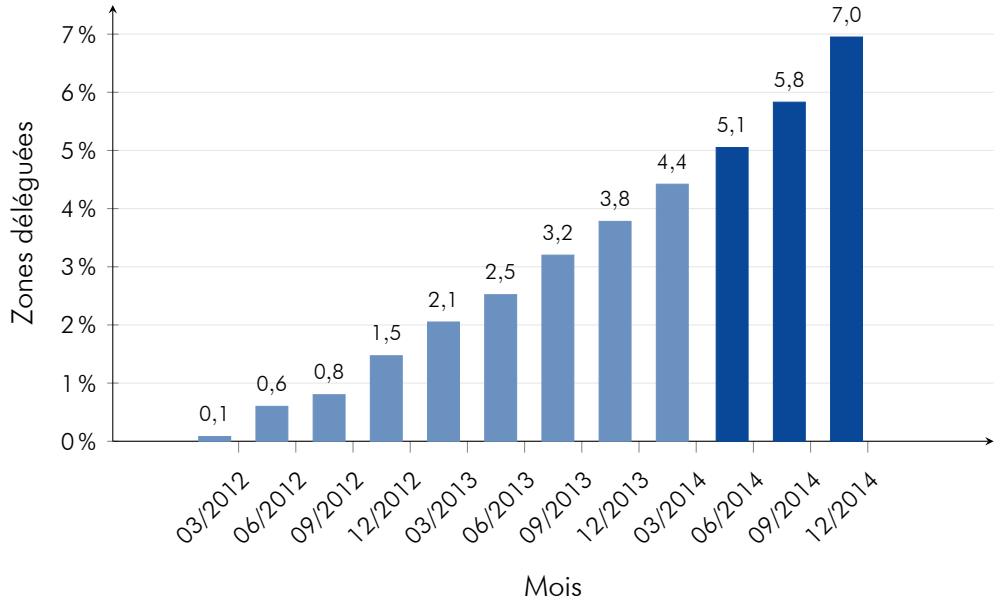


Figure 2.9 – Taux de zones signées de mars 2012 à décembre 2014 (par trimestre)

Fin décembre 2013, les zones possédant un DS se répartissaient entre 39 bureaux d'enregistrement. Le premier d'entre eux détenait à lui seul 97 % de ces zones. Le second n'en détenait que 0,7 %.

Une analyse similaire menée en décembre 2014 indique une évolution majeure. Ainsi, le nombre de bureaux d'enregistrement impliqués dans DNSSEC a doublé, passant à 85. Par ailleurs, le premier bureau fin 2013 détient désormais 87 % des zones. Il s'agit d'un résultat particulièrement intéressant qui montre que le déploiement DNSSEC est sorti de la phase d'expérimentation. Désormais, certains bureaux d'enregistrement

8. Delegation Signer.

ont des parts importantes de leurs portefeuilles de noms de domaine possédant un enregistrement DS.

Ces résultats s'expliquent principalement à la lumière de deux phénomènes. Le premier est le programme de nouveaux gTLD [9] réalisé par l'ICANN en 2014, pour lesquels DNSSEC est obligatoire. Le second est la campagne de promotion DNSSEC [27] lancée par l'Afnic qui permet aux bureaux d'enregistrement participants d'obtenir une remise sur le tarif de créations et de renouvellements de noms de domaines signés. Cette incitation financière a convaincu certains bureaux d'enregistrements de signer la quasi-intégralité de leur portefeuille de noms de domaine.

À retenir

Le protocole DNSSEC reste assez peu utilisé par les zones déléguées sous `.fr`. Cependant, la croissance constante du taux de zones possédant un enregistrement `DS` et l'implication significative de plusieurs bureaux d'enregistrement laisse prédire le maintien de cette dynamique de croissance en 2015 et l'implication d'un nombre grandissant de nouveaux bureaux d'enregistrement.

9. generic Top Level Domain.

2.5 Taux de pénétration d'IPv6

Les zones déléguées sous `.fr`

En 2014, le nombre de zones ayant au moins un serveur compatible IPv6 s'est stabilisé autour de 65 %, contre 63 % en 2013.

En revanche, pour les zones ayant tous leurs serveurs (DNS, mail et web) compatibles IPv6, leur taux reste faible comme les années précédentes. Il passe de 0,7 % en 2013, à 1,3 % en 2014.

Le taux de déploiement d'IPv6 s'est stabilisé pour les serveurs DNS et les serveurs de messagerie, comme l'illustre la figure 2.10. C'est d'ailleurs au niveau des serveurs DNS que le protocole IPv6 est le plus déployé pour les zones déléguées sous `.fr` avec plus de deux tiers des zones ayant au moins un serveur DNS répondant en IPv6.

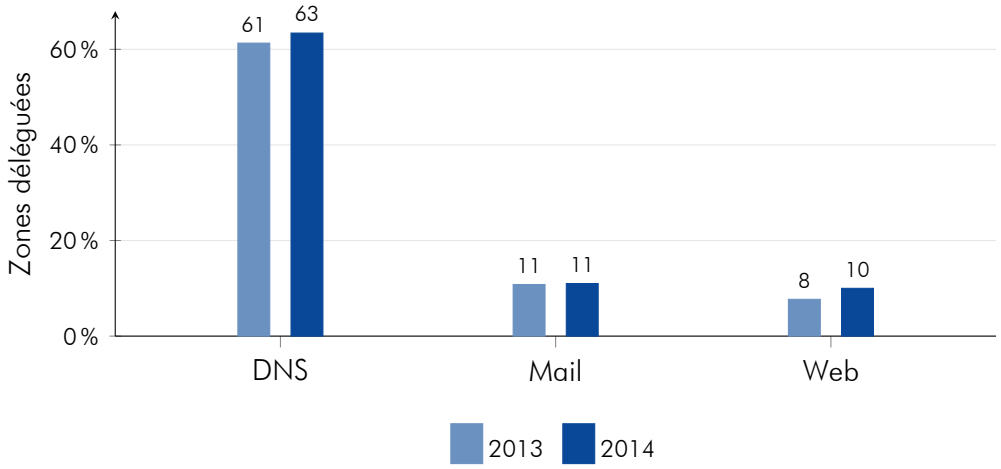


Figure 2.10 – Progression des serveurs compatibles IPv6 entre 2013 et 2014

Il est important de souligner que le taux de zones ayant au moins un service IPv6 est légèrement supérieur au taux de serveurs DNS compatibles IPv6. En effet, une faible proportion de zones n'a pas de serveur DNS IPv6, mais possède un serveur de messagerie ou un serveur web en IPv6.

Le taux de zones ayant au moins un serveur web IPv6 a continué sa progression en 2014, passant la barre des 10 %. Ce chiffre est à mettre en perspective avec celui des 1000 sites les plus populaires identifiés par la société Alexa. Selon les chiffres publiés par l'ISOC [10] [28], 14 % d'entre eux sont accessibles en IPv6.

10. Internet Society.

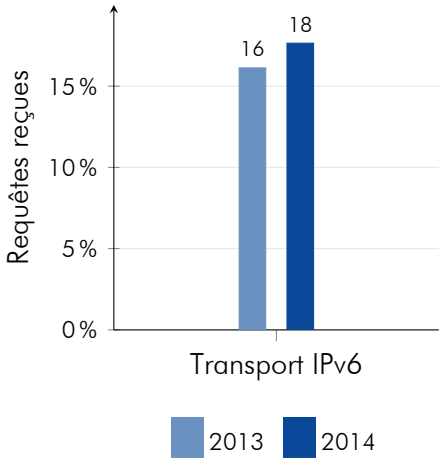


Figure 2.11 – Progression du transport IPv6 entre 2013 et 2014

Les requêtes DNS reçues

Le type de transport DNS observé par les serveurs faisant autorité donne une indication du taux d'activation d'IPv6 dans les résolveurs, alors que le type de données demandées (ex : requêtes de type `A`, `AAAA`, etc.) reflète le choix des machines utilisateurs.

Pour les serveurs faisant autorité pour `.fr` et étant directement administrés par l'Afnic, environ 18 % des requêtes sont transportées en IPv6 (voir figure 2.11) en décembre 2014. Le taux de pénétration d'IPv6 dans le transport du trafic DNS n'a donc pratiquement pas évolué entre 2013 et 2014.

Quant aux types de données demandées, le taux de requêtes demandant des adresses IPv6 a également stagné entre 2013 et 2014. En revanche, le taux de requêtes demandant des adresses IPv4 a légèrement augmenté sur cette même période au détriment des autres types de requêtes (`MX`, `DNSKEY`, `ANY`, etc.).

À retenir

La progression d'IPv6 en France, vu du DNS, a globalement stagné durant l'année 2014. Seul le déploiement d'IPv6 pour le service web a progressé, de façon modeste.

Conclusion générale

L'année 2014 a été marquée par de nombreuses activités malveillantes utilisant le protocole BGP comme vecteur pour détourner du trafic. En début d'année, une campagne d'usurpations de préfixes contre plusieurs hébergeurs a été utilisée pour voler des *bitcoins* [17]. De même, de juillet à novembre, un *spammeur* [18] a utilisé des usurpations afin de contourner les mécanismes de réputation d'adresses IP mis en œuvre dans le filtrage des courriers électroniques non sollicités. L'observatoire a également identifié cinq campagnes dont les caractéristiques semblent indiquer qu'il s'agit d'usurpations de préfixes contre des AS français. Une redirection de trafic a par ailleurs été mise en évidence par les mesures actives effectuées à l'aide des sondes Atlas [13].

Dès sa création, l'observatoire s'est attaché à mesurer l'utilisation de deux mécanismes de protection des protocoles DNS et BGP. L'année 2014 a connu des évolutions significatives. Ainsi, le nombre de bureaux d'enregistrement impliqués dans DNSSEC a doublé, sous l'impulsion de l'Afnic, passant à 85 en un an. De même, le nombre de zones signées s'est élevé à près de 7 % de la zone `.fr`. Pour la RPKI, le nombre d'AS français impliqués a lui aussi doublé, pour s'établir à 200 en fin d'année. Ce résultat est très encourageant, bien que les mesures effectuées ne permettent pas de déterminer si la RPKI est réellement utilisée pour filtrer des annonces BGP.

Concernant le protocole IPv6, l'observatoire a mis en évidence plusieurs changements remarquables. Tout d'abord, une augmentation de la concentration des interconnexions, marquée notamment par un nombre plus réduit d'AS pivots, comparé à l'année 2013. L'application des bonnes pratiques BGP se confirme avec la baisse du nombre d'AS français sans objets `route6` déclarés. Finalement, la progression d'IPv6 en France perçue à travers le protocole DNS a stagné en 2014. Seul le nombre de services web accessibles en IPv6 a augmenté de manière modeste.

Ce nouveau rapport présente, de surcroît, les premiers résultats concernant la résilience de la messagerie électronique à travers le protocole DNS. L'observatoire a ainsi identifié qu'un seul relais de messagerie entrant est configuré pour 42 % des zones déléguées sous `.fr`. La défaillance de ce relais serait donc critique pour la réception des messages électroniques. Par ailleurs, 51 % des relais sont fortement concentrés sur deux plateformes d'hébergement. Il s'agit d'un résultat important pour la résilience, qui est à mettre en perspective avec la concentration du marché de l'hébergement DNS, dans lequel quatre acteurs gèrent 70 % des serveurs.

Au regard des analyses concernant l'année 2014, l'observatoire renouvelle ses encouragements aux acteurs de l'Internet concernant l'appropriation des bonnes pratiques

d'ingénierie admises pour les protocoles BGP [1] et DNS [2]. D'autre part, l'observatoire énonce les recommandations suivantes :

- **surveiller les annonces de préfixes**, et se tenir prêt à réagir en cas d'usurpation ;
- **diversifier le nombre de serveurs SMTP et DNS** afin d'améliorer la robustesse de l'infrastructure ;
- **appliquer les bonnes pratiques** pour limiter les effets des pannes et des erreurs d'exploitation ;
- **poursuivre les déploiements** d'IPv6, de DNSSEC, et de la RPKI, afin de développer les compétences et d'anticiper d'éventuels problèmes opérationnels.

À retenir

Les organismes souhaitant participer à l'observatoire peuvent s'adresser à l'ANSSI et à l'Afnic.

Bibliographie

[1] ANSSI, "Bonnes pratiques de configuration de BGP," tech. rep., 2013.

[2] ANSSI, "Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine," tech. rep., May 2014.

[3] "Disco MapReduce," tech. rep., 2015.

[4] Valadon, Guillaume and Vivet, Nicolas, "Detecting BGP hijacks in 2014," PacSec and NSC, 2014.

[5] ANSSI, "Comprendre et anticiper les attaques DDoS," tech. rep., 2015.

[6] 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, 6793.

[7] M. Lepinski, Ed., "BGPSEC Protocol Specification - draft-ietf-sidr-bgpsec-protocol-12." <http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-12>, 2014.

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

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

[10] O. Tange, "Gnu parallel - the command-line power tool," *;login : The USENIX Magazine*, vol. 36, pp. 42–47, Feb 2011.

[11] "asrank - Implementation of CAIDA AS ranking algorithm," tech. rep., Feb. 2014.

[12] M. Luckie, B. Huffaker, k. claffy, A. Dhamdhere, and V. Giotsas, "AS Relationships, Customer Cones, and Validation," in *Internet Measurement Conference (IMC)*, October 2013.

[13] RIPE-NCC, "RIPE Atlas." <https://atlas.ripe.net/>.

[14] DynResearch, "The new threat : Targeted internet traffic misdirection." <http://research.dyn.com/2013/11/mitm-internet-hijacking/>, November 2013.

[15] DynResearch, "Indonesia hijacks the world." <http://research.dyn.com/2014/04/indonesia-hijacks-world/>, April 2014.

[16] BGPMON, "Bgp hijack incident by syrian telecommunications establishment." <http://www.bgpmon.net/bgp-hijack-incident-by-syrian-telecommunications-establishment/>, December 2014.

[17] D. SecureWorks, "Bgp hijacking for cryptocurrency profit." <http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/>, August 2014.

[18] DynResearch, "The vast world of fraudulent routing." <http://research.dyn.com/2015/01/vast-world-of-fraudulent-routing/>, January 2015.

[19] P. Mockapetris, "Domain names - concepts and facilities." RFC 1034 (INTERNET STANDARD), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

[20] P. Mockapetris, "Domain names - implementation and specification." RFC 1035 (INTERNET STANDARD), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.

[21] IANA, "Domain Name System (DNS) Parameters." <http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml>.

[22] "Observatoire de la Résilience de l'Internet français - rapport 2013." <http://www.ssi.gouv.fr/observatoire>, Sept. 2013.

[23] Afnic, "DNSwitness." <http://www.dnswitness.net/>.

[24] "Observatoire du marché des noms de domaine en France." <https://www.afnic.fr/fr/ressources/publications/observatoire-du-marche-des-noms-de-domaine-en-france/>, 2014.

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

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

[27] "L'Afnic s'engage dans la promotion de DNSSEC." <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/7380/show/l-afnic-s-engage-dans-la-promotion-de-dnssec-2.html>, Nov. 2013.

[28] ISOC, "Percentage of Alexa Top 1000 websites currently reachable over IPv6." <http://http://www.worldipv6launch.org/measurements/>, July 2014.

Acronymes

Afnic	Association Française pour le Nommage Internet en Coopération
ANSSI	Agence nationale de la sécurité des systèmes d'information
AS	Autonomous System
BGP	Border Gateway Protocol
BGPsec	Border Gateway Protocol Security
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	DNS SECurity extensions
DS	Delegation Signer
FAI	Fournisseur d'Accès à Internet
gTLD	generic Top Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés
IP	Internet Protocol
IRR	Internet Routing Registry
ISOC	Internet Society
RIPE-NCC	RIPE Network Coordination Centre
RIR	Regional Internet Registry
RIS	Routing Information Service
ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure
SPOF	Single Point Of Failure

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.

Septembre 2015

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