Résilience de l'Internet français

2015

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, Pierre Lorinquer, Florian Maury, Julie Rossi, Maxence Tury, 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. 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 contenant pas les acteurs étrangers.
La résilience se définit comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Elle peut être caractérisée par des indicateurs mesurables dont certains sont directement issus de règles d'ingénierie appelées bonnes pratiques.

Rédigé par l'ANSSI [1], ce rapport analyse la résilience à travers les protocoles BGP [2], DNS [3], et TLS [4]. Les deux premiers permettent respectivement d'acheminer des données à l'aide d'annonces de routage, et de fournir la correspondance entre un nom de domaine et une adresse IP. Le troisième est notamment utilisé pour chiffrer les communications entre un serveur web et ses clients.

En 2015, l'observatoire a identifié que la version recommandée TLS 1.2 est prise en charge par 75 % des serveurs web de zones déléguées sous `.fr`. Concernant le protocole IPv6, les tendances amorcées les années précédentes se confirment, indiquant que les bonnes pratiques d'exploitation de ce protocole semblent peu suivies. Afin de permettre la reproduction d'une partie des résultats, les principaux outils utilisés pour les analyses BGP ont été publiés [1, 2].

L'observatoire encourage l'ensemble des acteurs de l'Internet à s'approprier les bonnes pratiques d'ingénierie admises pour les protocoles BGP [3], DNS [4], et TLS, et à anticiper la menace que représentent les DDoS [5]. D'autre part, l'observatoire énonce les recommandations suivantes :

- **surveiller les annonces de préfixes** et se tenir prêt à réagir aux usurpations ;
- **utiliser des algorithmes supportant la confidentialité persistante**, et **abandonner SSLv2 et SHA-1** au profit de mécanismes plus robustes ;
- **diversifier le nombre de serveurs SMTP et DNS** afin d'améliorer la robustesse de l'infrastructure ;
- **appliquer les bonnes pratiques** notamment celles rappelées dans ce document, 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. Border Gateway Protocol.
3. Domain Name System.
4. Transport Layer Security.

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 l'économie française. 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 difficiles à identifier. En raison de l'importance de cette problématique, la nécessité de créer un organisme chargé d'étudier les risques de dysfonctionnement de l'Internet au niveau national s'est imposée.

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 susceptibles d'entraver 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 aussi complète que 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 frontières. 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 sur le territoire. Dans le cadre de ses études, l'observatoire se concentre 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 à limiter en amont et 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 l'adoption la plus large possible des bonnes pratiques admises.

Introduction

Forte de son expérience sur les protocoles BGP et DNS, l'équipe de l'observatoire a souhaité étendre ses analyses à d'autres protocoles afin de mieux comprendre l'Internet français. Ainsi, le choix s'est porté sur le protocole TLS qui permet, notamment, de chiffrer les communications entre un serveur web et ses clients. Le périmètre de cette nouvelle analyse se compose de l'ensemble des sites web correspondants aux zones déléguées sous `.fr` qui mettent en œuvre HTTPS [5]. Ce nouveau rapport présente différents indicateurs et leurs méthodologies de mesure, ainsi que les résultats associés aux observations faites sur TLS.

En ce qui concerne le protocole BGP, les principaux outils utilisés pour les analyses ont été publiés [1, 2]. Ils permettent à la fois d'analyser les archives BGP du projet RIS [6], et de détecter les conflits d'annonces de préfixes [6]. Au cours de l'année 2015, une nouvelle méthodologie de détection des réannonces de routes a par ailleurs été développée. Elle a pour objectif de faciliter les analyses manuelles tout en réduisant le nombre de faux positifs. Il s'agit d'une étape importante dans l'automatisation des tâches répétitives de classification effectuées manuellement jusqu'alors.

L'étude des relais de messagerie via le protocole DNS, introduite dans le rapport 2014, a été améliorée, notamment vis-à-vis des dépendances à des noms de domaines tiers, et des dispersions par pays et par opérateurs. Cette évolution permet de mieux appréhender les phénomènes de concentration sur des plateformes d'hébergement qui peuvent affecter la disponibilité des services. Pour faire écho au nouvel indicateur sur le protocole TLS, les observations sur DNSSEC incorporent désormais une analyse des algorithmes cryptographiques utilisés.

Par souci de concision, ce nouveau rapport présente une synthèse des analyses, et détaille les éléments marquants de l'année 2015. Les rapports précédents font ainsi référence en ce qui concerne les descriptions et les méthodologies des indicateurs techniques étudiés.

À retenir

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

5. La version du protocole HTTP protégée par TLS.
6. Routing Information 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 [7]. L'objectif de ce protocole est d'échanger des informations de joignabilité de préfixes entre deux opérateurs qui sont alors appelés AS[2] et 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

1. Internet Protocol.
2. Autonomous System.

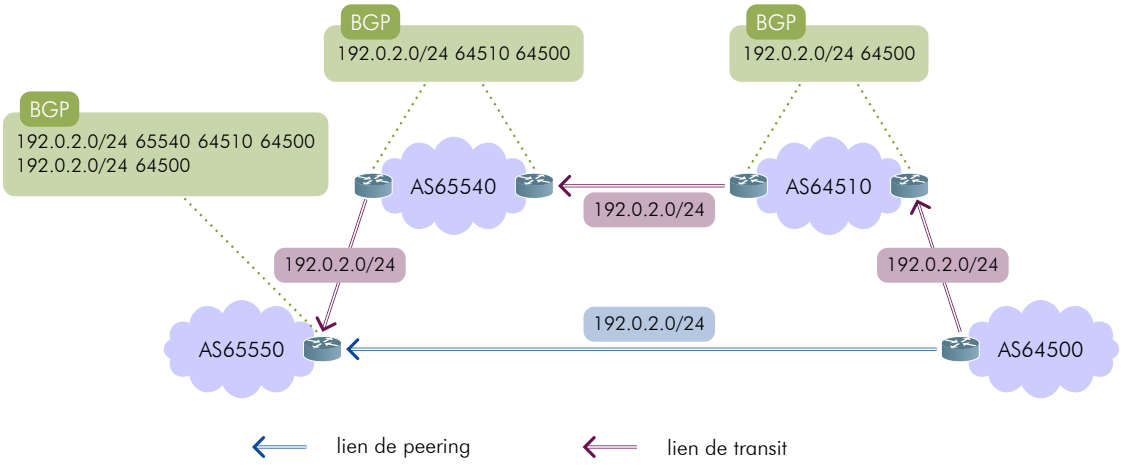


Figure 1.1 – Exemple de chemins d'AS sur des liens de transit et peering

conséquent, un AS malveillant peut annoncer un préfixe appartenant à un autre AS. 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 [3] 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`

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

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 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, comme certaines formes de protection anti-DDoS, 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, ainsi, de se prémunir contre des 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] [8], est toujours 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] [9] 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'entre 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

Afin d'étudier la résilience sous l'angle de BGP, l'observatoire utilise les données BGP archivées par le projet RIS [10]. Treize routeurs spécifiques, appelés collecteurs, enre-

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.

gistrent en temps réel l'ensemble des messages BGP reçus de leurs pairs. La répartition géographique de ces collecteurs permet d'obtenir la vision locale de l'Internet d'une centaine d'AS à travers le monde, principalement en Amérique du Nord et en Europe.

Les informations de routage sont analysées par l'observatoire avec des outils dédiés, dont certains ont été publiés en source ouverte. Ainsi, la transformation des messages binaires BGP dans un format textuel intermédiaire est assurée par l'outil *MaBo* [1]. La détection d'usurpation de préfixes est réalisée par *TaBi* [2] et l'étude de la connectivité des AS par l'outil *AS Rank* [11].

L'industrialisation de ces outils a également fait l'objet d'un travail important par l'équipe de l'observatoire, dans le but de produire les indicateurs plus souvent et sans intervention manuelle. Ainsi, l'exécution des tâches régulières, comme la récupération des archives BGP ou des dépôts `whois` et RPKI [12], est effectuée à l'aide de la bibliothèque `luigi` [13]. De plus, certaines tâches, dont le temps de traitement est trop important, sont exécutées sur une plateforme de calculs distribués mettant en œuvre le logiciel `disco` [14].

Entre 2013 et 2014, l'observatoire a expérimenté l'usage de mesures actives pour tenter de mieux qualifier les usurpations de préfixes. La corrélation des informations du plan de donnée avec des informations de routage provenant du plan de contrôle donne des résultats intéressants. Néanmoins, cette expérimentation n'a pas été reconduite en 2015 car le RIS [10] et le réseau de sondes `Atlas` induisent une latence de quelques minutes. L'observatoire continue de travailler avec le RIPE-NCC pour rendre la prise de mesures en temps réel possible.

À retenir

En 2015, l'observatoire a identifié 1588 AS français. Parmi ceux-ci, le nombre d'AS visibles est de 1001 à la fin du mois de décembre 2015, contre 880 fin décembre 2014.

1.1.5 Évolution des AS français

En 2015, à l'aide de la méthode définie dans les précédents rapports, l'observatoire a identifié 1588 AS français. Parmi ceux-ci, 1001 sont visibles dans les archives BGP, c'est-à-dire qu'ils ont annoncé au moins un préfixe pendant l'année.

Un noyau dur de 869 AS actifs annonce au moins un préfixe par jour tout au long de l'année 2015, ce qui représente environ 87 % du nombre total d'AS distincts visibles au cours de l'année. Parmi les 13 % d'AS visibles restant, environ 50 % d'entre eux l'ont été pendant la moitié de l'année. Enfin, 587 AS répertoriés n'ont pas annoncé de préfixe en 2015.

1.2 Connectivité des AS français

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

À titre d'exemple, les représentations graphiques de la connectivité en IPv4 et en IPv6 sont données dans les figures 1.3 et 1.4. 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 de mettre en évidence les « AS pivots ». Il s'agit d'AS dont la panne totale entraînerait la perte de connectivité à l'Internet pour des AS français. Ils apparaissent en vert et orange dans les figures. Pour IPv6, il est intéressant de noter que le graphe de connectivité comporte beaucoup moins d'AS qu'en IPv4.

Évolution de l'Internet français

Les graphes de connectivité fournissent des informations permettant d'étudier la dynamique de l'Internet au cours de l'année 2015. La figure 1.5 montre ainsi, qu'en IPv4, le nombre d'AS français est passé de 905 à 970. Le rythme de croissance est ainsi de 7 %. Soit un nombre très proche de celui observé en 2014. En IPv6, il est de 13 %, contre 6 % l'année précédente ; le nombre d'AS français est de 304 en fin d'année.

L'Internet français dépend d'AS étrangers pour faire transiter le trafic entre certains 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`. La figure 1.5 montre, qu'en IPv4, leur nombre a crû lentement tout au long de l'année pour atteindre 293, un nombre légèrement inférieur à celui observé en 2014. En IPv6, comme en 2013 et 2014, une cinquantaine d'AS étrangers sont nécessaires pour interconnecter tous les AS français.

Impacts de la disparition d'un AS

En IPv4, les nombres d'AS pivots français et étrangers sont restés stables comme le montre la figure 1.6. À l'inverse, en IPv6, le nombre d'AS pivots français a très légèrement augmenté, atteignant 40 en fin d'année. Ce changement de tendance par rapport à 2014 pourrait s'expliquer par de nouveaux déploiements d'IPv6 par les AS français.

L'impact de la panne d'AS pivots est un élément important qui permet d'évaluer la robustesse de la connectivité. La figure 1.7 montre qu'en IPv4, seuls 7 AS pivots affec-

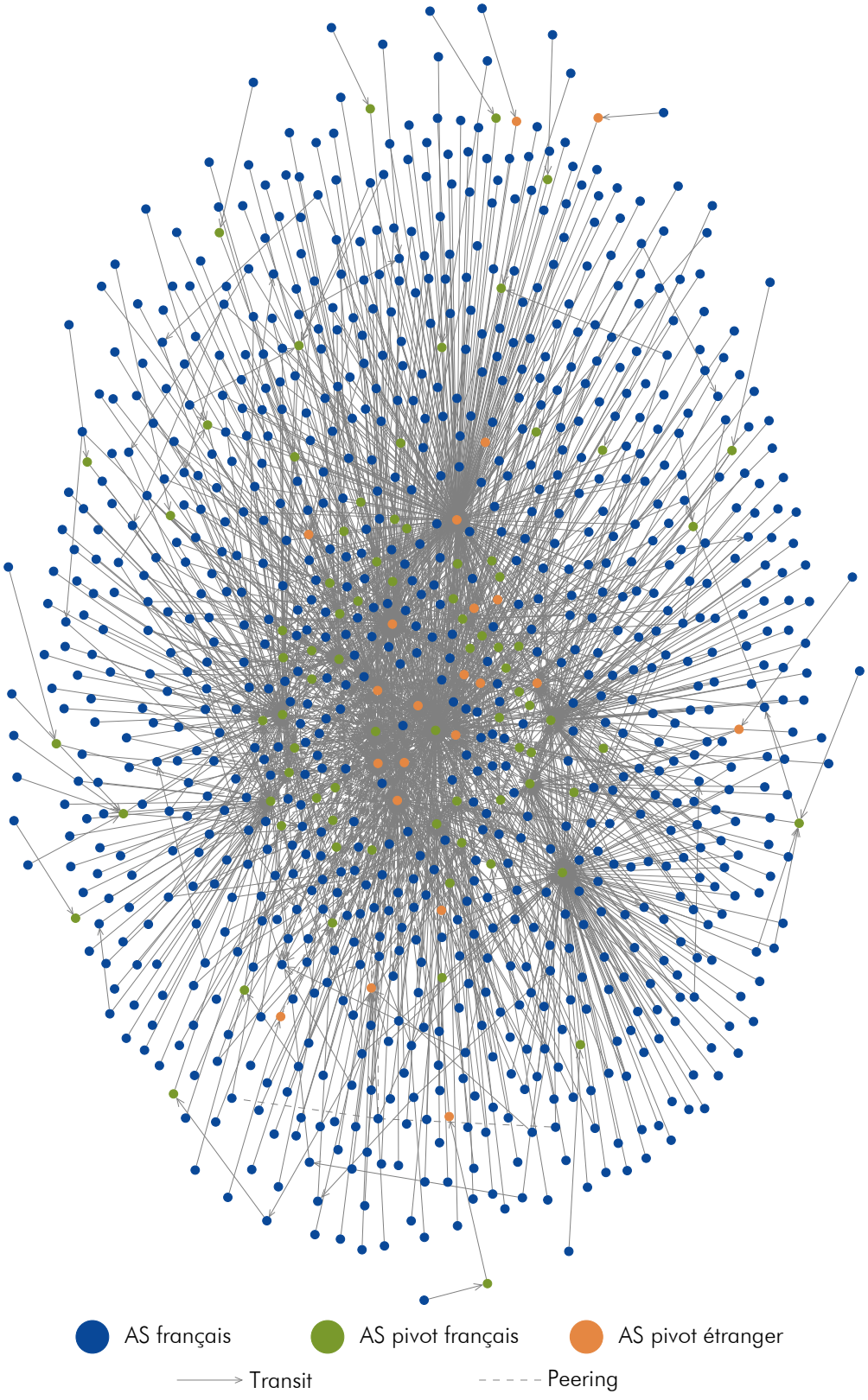


Figure 1.3 – Graphe de connectivité en IPv4 (décembre 2015)

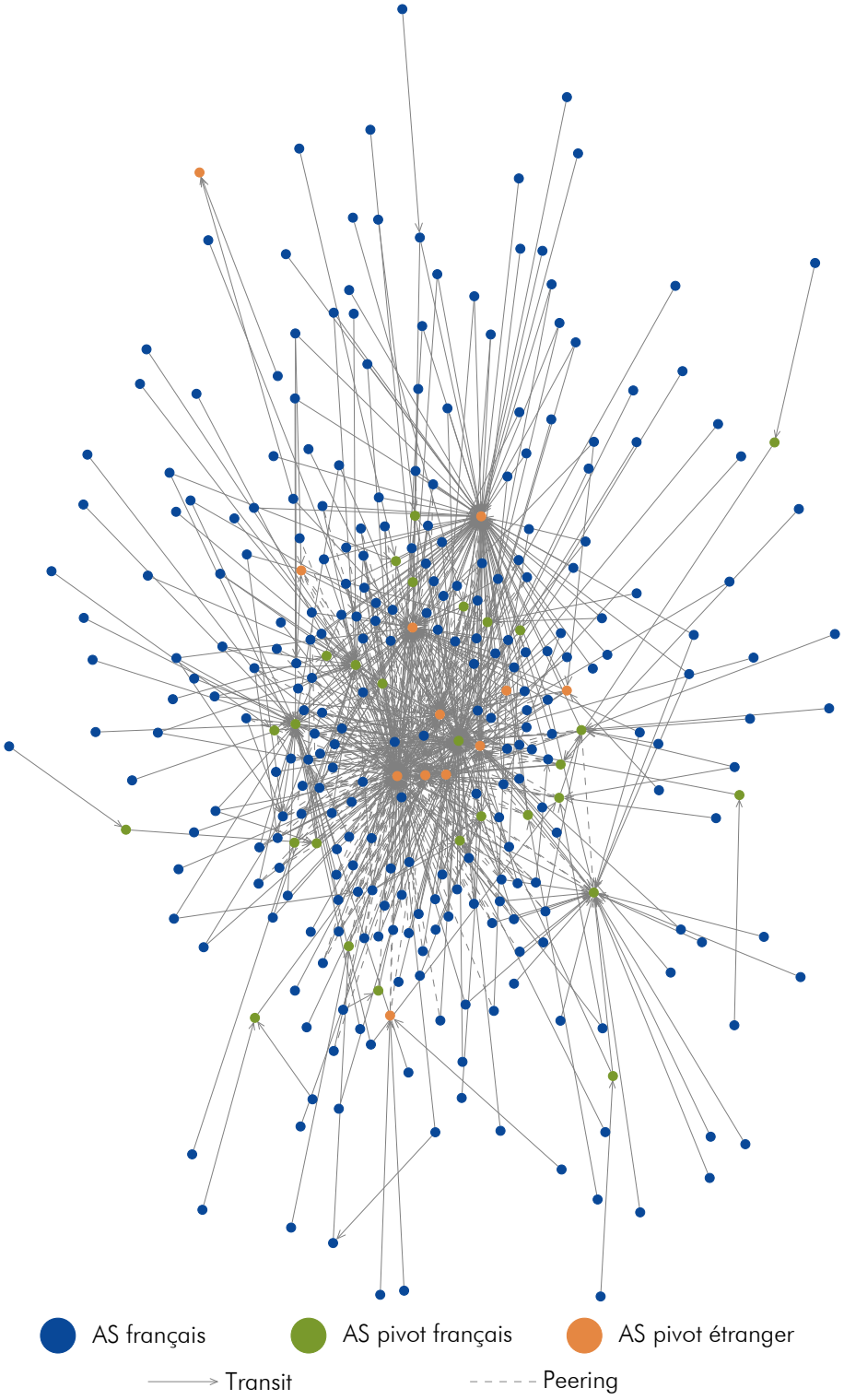


Figure 1.4 – Graphe de connectivité en IPv6 (décembre 2015)

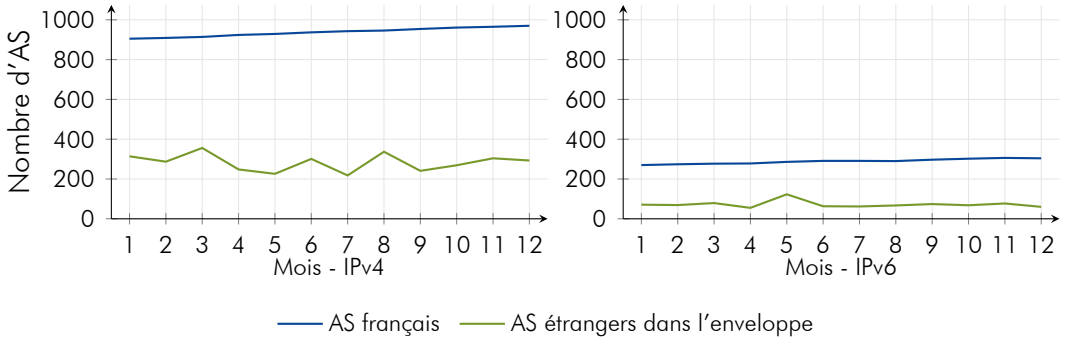


Figure 1.5 – Évolution du nombre d'AS français et de l'enveloppe en 2015

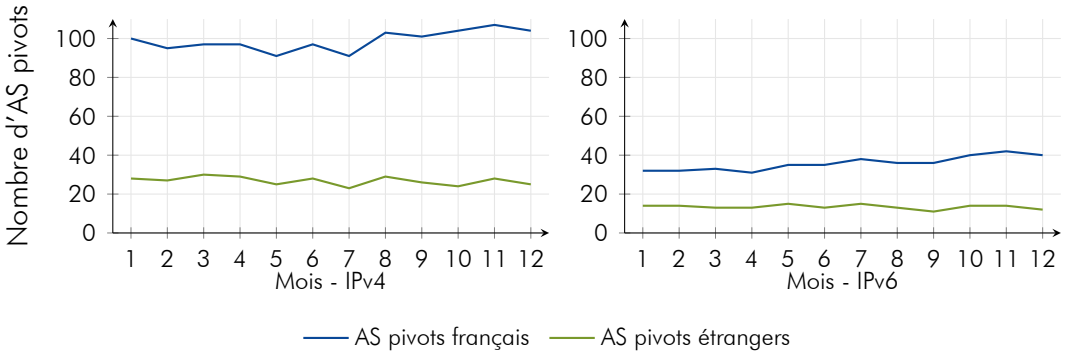


Figure 1.6 – Évolution du nombre d'AS pivots français et étrangers en 2015

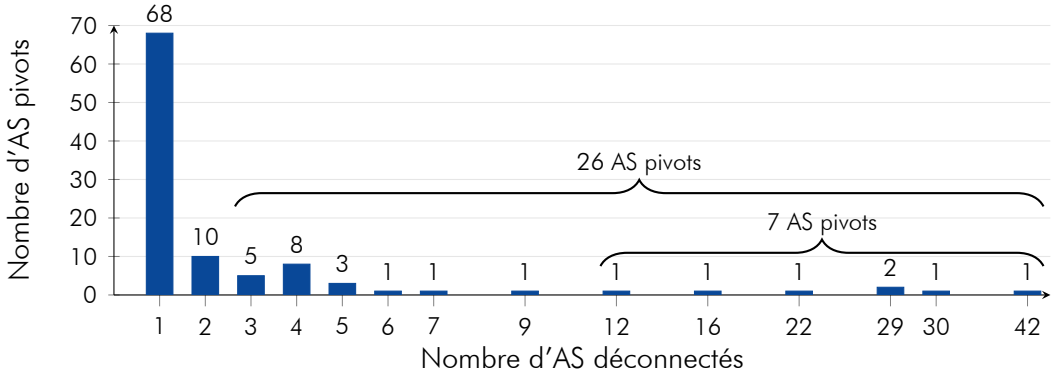


Figure 1.7 – AS pivots en fonction du nombre d'AS déconnectés (IPv4, déc 2015)

teraient au moins 10 AS en cas de défaillance. Il s'agit d'une légère amélioration par rapport à 2014. En revanche, l'AS pivot le plus critique aurait un impact sur 42 AS, contre 35 en 2014. Ce résultat, sans être dramatique, pointe cependant la nécessité d'être vigilant quant aux évolutions de dépendance des AS.

Pour IPv6, la figure 1.8 montre qu'il existe moins d'AS pivots qu'en IPv4. Cependant, vis-à-vis de 2014, le nombre d'AS pouvant être déconnectés a augmenté. Il s'agit d'un

résultat intéressant qui découle naturellement de l'évolution de l'Internet IPv6 français, et de la croissance du nombre d'AS IPv6 pivots.

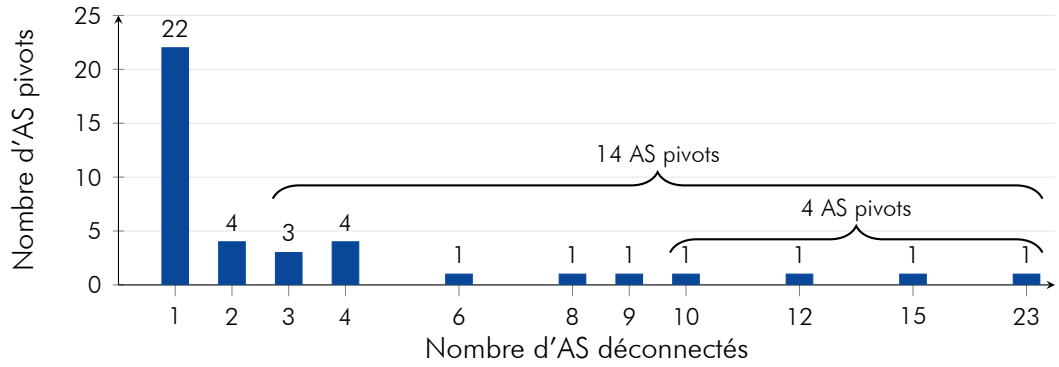


Figure 1.8 – AS pivots en fonction du nombre d'AS déconnectés (IPv6, déc 2015)

À retenir

En IPv6, le nombre d'AS a augmenté de 13 % en 2015, contre 6 % l'année précédente. Le nombre d'AS pivots a quant à lui légèrement augmenté. Cela semble indiquer un accroissement du déploiement d'IPv6 par les AS français.

1.3 Usurpations de préfixes

Résultats globaux

En 2015, l'observatoire a détecté 6392 conflits d'annonces. Ils ciblent 344 AS français distincts, et 1350 préfixes. Leur classification est fournie dans la figure 1.9. Près de 50 % d'entre eux sont des annonces légitimes validées par des objets `route` ou des `ROA`. Environ 2 % des conflits sont uniquement validés par des `ROA`.

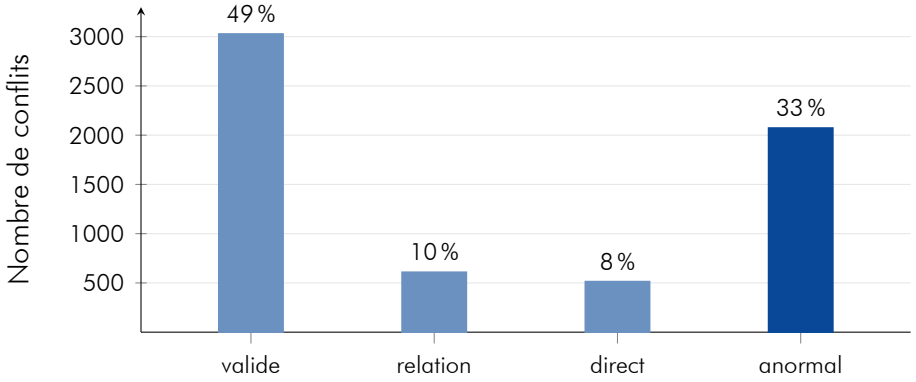


Figure 1.9 – Types de conflits détectés en 2015

Les catégories « relation » et « direct » permettent quant à elles d'éliminer 18 % des conflits. Ces validations simples, basées sur les liens techniques et commerciaux entre AS, sont néanmoins efficaces pour limiter le nombre de conflits qui ne sont pas des usurpations. Ainsi, seuls 2070 conflits anormaux seront considérés lors de l'identification des usurpations.

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 importants, et trouvent leur origine auprès d'un même AS sur une courte période.

L'observatoire a développé un algorithme dans le but de détecter automatiquement ces réannonces de table globale. Il vise à modéliser une réannonce de table globale comme un événement au cours duquel il y a simultanément et sur une courte durée une augmentation significative du nombre de préfixes annoncés par un AS et du nombre d'AS en conflit avec cet AS. La corrélation de ces deux critères permet de travailler avec des valeurs faibles pour détecter des pics, évitant ainsi d'écarter à tort certains cas.

Au cours de l'année 2015, l'algorithme a détecté plusieurs milliers d'AS ayant des pics d'annonces de préfixes et plusieurs centaines d'AS ayant des pics de nombre d'AS en

conflit. Une fois la corrélation effectuée, seuls 35 AS sont à l'origine de réannonces de table globale.

Certains AS ayant fait des réannonces plusieurs fois en 2015, ces résultats correspondent à 38 réannonces de table globale dans l'année, soit plus de 3 par mois. Parmi ces 35 AS, seulement 14 ont été en conflit avec des AS français aux dates où les réannonces de table globale ont été détectées, impactant 175 AS français au total.

En particulier, le 27 octobre de 10h à 11h, un AS de Hong Kong a annoncé plus de 15 000 préfixes supplémentaires, entrant en conflit avec plus de 6000 AS dont 93 français. Le second est un AS indien [15] qui a annoncé, le 6 novembre, près de 30 000 préfixes supplémentaires, entrant en conflit avec plus de 3000 AS dont 36 français entre 6h et 16h. Le troisième est un AS grec qui a annoncé, le 9 octobre à 13h, près de 30 000 préfixes supplémentaires, entrant en conflit avec plus de 3000 AS dont 33 français. Les 11 autres sont entrés en conflit avec moins de 20 AS français.

L'algorithme utilisé est restrictif et tend à minimiser le nombre de faux positifs au détriment du nombre de faux négatifs. Une analyse manuelle a confirmé que le nombre total de réannonces de table globale dépasse les 38 détectées. En effet, certains événements [16] n'ont pas été détectés en raison de leur faible impact sur l'Internet français ou de leur apparition décorrélée de la réannonce détectée [15]. Sur les 2070 conflits anormaux, 1480 conflits correspondent à des réannonces de table globale.

À retenir

En 2015, l'observatoire a identifié 35 AS à l'origine de réannonces de table globale.

Protection contre les DDoS

Au cours de l'année 2015, la menace des attaques DDoS est restée importante pour les AS français. Différentes techniques [5] existent afin d'en limiter les impacts. L'une d'elles est basée sur BGP et se caractérise par des annonces de préfixes effectuées par un opérateur spécialisé, à la place de l'AS attaqué. Dans les données BGP, cette technique est vue comme un conflit d'annonces.

L'objectif est en effet de détourner le trafic vers l'opérateur spécialisé qui possède une importante capacité de débit, et des équipements permettant à la fois de dépolluer le trafic, et de protéger les adresses IP de destination. En pratique, l'opérateur spécialisé annonce des préfixes plus spécifiques [12] que ceux annoncés par le client qu'il protège, afin de récupérer l'ensemble du trafic. Une fois la dépollution effectuée, le trafic légitime peut, par exemple, être envoyé au client dans un tunnel.

12. Habituellement des préfixes /24.

Au cours de l'année 2015, l'observatoire a mis en évidence 149 conflits anormaux qui correspondent à des protections contre les DDoS, allant de quelques heures à plusieurs mois. Les AS français protégés sont de natures différentes, comme des hébergeurs, des assurances, ou des sites de paris en ligne. Il est intéressant de souligner qu'aucun des opérateurs spécialisés utilisés n'était français.

À retenir

Près de 150 conflits anormaux correspondant à des mécanismes de protection contre les DDoS ont été mis en évidence en 2015.

Filtrage automatique des conflits anormaux

Afin de faciliter les analyses manuelles, l'observatoire a amélioré ses capacités de détection automatique des usurpations de préfixes. Ainsi, un nouveau filtre identifie automatiquement des relations entre AS en étudiant la proximité de leurs noms. Cela permet par exemple de mettre en évidence des conflits entre un AS étranger et ses filiales françaises. De même, un filtre similaire est utilisé pour identifier des fautes de frappe dans les numéros d'AS lors des configurations d'interconnexion BGP.

Les conflits anormaux portant sur des préfixes réservés [13] ou trop spécifiques sont filtrés car il est difficile d'en déterminer l'origine. Ceux issus de numéros d'AS spéciaux [14] le sont également. Cette étape permet d'écarter environ 250 conflits anormaux.

Le filtre suivant consiste à identifier les conflits anormaux entre deux AS pour lesquels il existe des conflits d'une autre catégorie. Si des conflits sont validés par des objets `route` pour certains préfixes, mais pas pour d'autres, il existe probablement une relation forte entre les deux AS. Environ 80 conflits anormaux sont filtrés de cette façon.

Finalement, des filtres portant sur la durée des conflits, leur visibilité par les collecteurs du RIS, et le pays de l'AS usurpateur sont appliqués. Ceux qui durent plus de deux mois, et qui sont visibles par moins de 10 pairs du RIS sur 120, sont filtrés. Les conflits issus d'AS français le sont également. Près de 250 conflits supplémentaires sont ainsi écartés.

Le filtrage basé sur la similarité des noms des AS a permis d'identifier 4 conflits entre un opérateur et sa filiale française. Celui sur les numéros d'AS a mis en évidence une erreur de configuration d'un routeur BGP ayant engendré 5 conflits distincts. Ces filtres automatiques limitent efficacement les analyses manuelles à effectuer. Seuls 89 conflits anormaux, doivent ainsi être étudiés attentivement.

13. Comme le préfixe 6to4 `2002::/16`.
14. Il s'agit des AS privés, de documentations, et de l'AS_TRANS.

Analyse manuelle

Une analyse manuelle permet de limiter fortement le nombre de conflits anormaux. En 2015, l'équipe de l'observatoire a mis en évidence une dizaine de conflits très courts correspondant à l'annonce des préfixes de points d'échanges par leurs membres. Il s'agit probablement d'erreurs de configuration car ces préfixes ne doivent en aucun cas être annoncés. Une vingtaine de conflits s'explique par les relations entre AS. Par exemple, un conflit touchant un opérateur français est effectué par sa filiale espagnole.

Cette année, une relation plus subtile a été mise en évidence. Deux AS étrangers distincts étaient en conflit avec un AS français. Pour l'un d'entre eux, un objet route avait été créé. Les noms de ces deux AS étant similaires, il s'agit probablement d'un défaut de déclaration d'objet route. Une recherche approfondie a permis de mettre en évidence la relation commerciale liant ces deux AS et l'AS français.

Enfin, les attributs optionnels `import` et `export` contenus dans les objets `aut-num` ont permis d'écarter 5 conflits. En effet, dans chacun des cas, il existait bien une relation commerciale entre les deux AS : l'un étant client de l'autre. Forte de ces nouvelles analyses manuelles, l'équipe de l'observatoire va pouvoir affiner les filtres automatiques mis en œuvre dans ses outils.

Usurpations de préfixes

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

À l'issue des analyses automatiques et manuelles, il reste 40 conflits anormaux qui pourraient être des usurpations de préfixes. Afin de réduire leur nombre, seuls les conflits anormaux comportant des annonces plus spécifiques sont conservés. Il apparait ainsi que 26 conflits anormaux correspondent à des usurpations dont les durées vont de cinq minutes à quatre jours.

Début juillet, un AS russe a été à l'origine de 5 conflits distincts ciblant un AS français. Ce comportement est suspect, et similaire aux observations effectuées en 2014 liées aux campagnes de *spam* [17]. Durant l'année, il a annoncé près de 150 préfixes différents ne lui appartenant pas. Parmi les autres conflits anormaux, une dizaine correspond très probablement à d'autres campagnes de *spam* utilisant BGP. Un AS roumain identifié dans le rapport précédent a effectué ce type d'usurpations en 2015.

Finalement, 15 conflits anormaux possèdent des caractéristiques semblant indiquer qu'il s'agit très probablement d'usurpations de préfixes ayant touché des AS 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. Cet indicateur porte sur l'analyse des 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 n'étant pas couvert par un objet `route`.

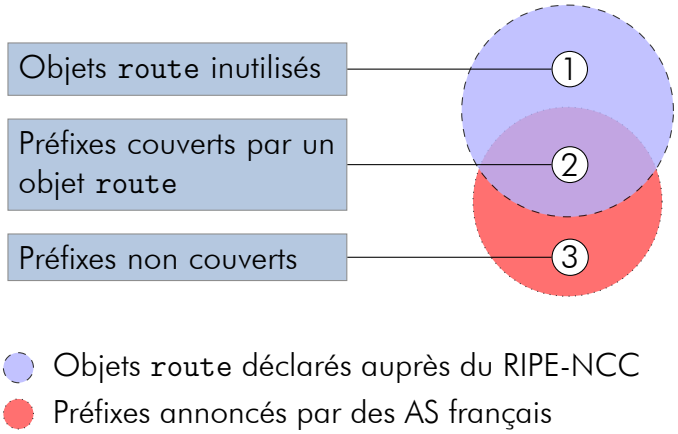


Figure 1.10 – Représentation des sous-indicateurs de l'utilisation des objets `route`

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. La tendance reste constante par rapport aux années précédentes. Au cours de l'année, 137 objets `route` orphelins se sont ajoutés aux 1556 présents au 1er janvier 2015. Pour IPv6, la quantité d'objets `route6` orphelins est passée de 182 à 232.

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	653	575
	aucun objet `route` utilisé	91	103
IPv6	aucun objet `route6` déclaré	1256	1195
	aucun objet `route6` utilisé	108	132

Table 1.1 – Répartition des AS selon l'usage des objets `route` en 2015

Afin d'analyser les AS du point de vue des objets `route` inutilisés, l'observatoire les classe dans deux catégories, représentées par le tableau 1.1 :

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

Les quantités d'AS n'ayant aucun objet `route` déclaré en 2015 diminuent respectivement de 78 et 61 AS pour IPv4 et IPv6. 575 AS en IPv4 et 1195 en IPv6 étaient dans cette catégorie au 31 décembre. Malgré ce nombre encourageant, le nombre d'AS n'utilisant aucun des objet `route` déclarés augmente de 12 en IPv4 et de 24 en IPv6, finissant au nombre de 103 en IPv4 et 132 en IPv6. Il est important de noter que la plupart de ces AS ont arrêté d'annoncer des préfixes sur Internet : il ne s'agit donc pas de nouveaux opérateurs ne respectant pas les bonnes pratiques vis-à-vis du RIPE-NCC.

Préfixes couverts par des objets route

Une interconnexion BGP peut faire l'objet d'un filtrage. La plupart du temps, ce filtrage se fait via une liste issue des objets `route` déclarés. Nous nous intéressons donc ici à mettre en évidence les préfixes et AS qui seraient couverts par de tels filtres.

La couverture des préfixes par des objets `route` s'améliore depuis 2011. Les préfixes IPv4 couverts par des objets `route` sont passés de 4211 à 4709 en 2016. En IPv6, 69 préfixes se sont ajoutés aux 358 présents au début de l'année.

Afin d'avoir une idée de la joignabilité des AS, ceux dont tous les préfixes sont couverts par des objets `route` sont étudiés. Pour IPv4, 726 AS entraient dans cette catégorie au 1er janvier ils étaient 805 au 31 décembre, soit une amélioration d'accessibilité pour 79 AS. Nous constatons que parmi ces AS, 77 sont des AS créés au cours de l'année. Les nouveaux AS tendent fortement vers l'application des bonnes pratiques. En IPv6, la situation est passée de 212 à 249 AS ayant tous leurs préfixes couverts par des objets `route6`. Dans cet ensemble d'AS, 15 ont été créés en 2015.

Préfixes non couverts par des objets route

Comme pour le sous-indicateur précédent, la situation continue de s'améliorer. De 841 préfixes IPv4 non couverts début 2016, l'année se termine avec 785 préfixes non couverts. Pour IPv6, le nombre de préfixes non couverts est passé de 121 à 125 en 2015. La situation se dégrade donc ici, et montre qu'il est nécessaire de renforcer les efforts sur ce protocole.

Enfin, nous considérons ici les AS pour lesquels au moins un des préfixes annoncés n'est pas couvert par un objet `route`. En IPv4, 171 AS étaient concernés au début de l'année. Au 31 décembre, ils étaient 163 dans cette situation. Pour IPv6, l'ensemble n'a que très peu varié : le nombre d'AS pour lesquels il manque au moins un objet `route6` est passé de 51 à 48 au cours de l'année 2015.

À retenir

Contrairement aux années précédentes, le nombre de préfixes IPv6 non couverts par des objets `route6` augmente.

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 que le nombre d'AS participants a crû au cours de l'année 2015. Au début du mois de janvier, 198 AS français avaient des ROA dans la RPKI. Au 31 décembre, la RPKI contient des déclarations issues de 237 AS français, ce qui représente une croissance de près de 20 %. On remarque que cette augmentation est bien plus faible que celle observée au cours de l'année précédente. En 2014, le nombre d'AS participant à la RPKI avait augmenté de près de 80 % entre le début du mois de janvier et la fin du mois de décembre.

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 2015 a été étudiée. Le pourcentage de l'espace d'adressage valide connaît peu d'évolution au cours de l'année. Au 31 décembre 2015, environ 65 % de l'espace d'adressage est valide selon la RPKI.

En parallèle, les pourcentages de l'espace d'adressage non couvert et de l'espace d'adressage invalide sont restés stables au cours de l'année. Au 31 décembre 2015, 34,4 % de l'espace d'adressage n'était 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 2015, ce pourcentage est de 0,4 %.

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 2015, les ROA couvraient moins de 1 % de cet espace d'adressage. Il n'y a donc pas eu d'évolution significative de cette couverture depuis 2014.

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 a également porté 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 2015. De 102 en janvier 2015, ce nombre passe à 118 à la fin de l'année. Par ailleurs, seul un AS a effectué uniquement des annonces de préfixe invalides au cours du mois de décembre 2015.

Ces résultats montrent qu'en cas de filtrage strict basé sur la RPKI, près de 12 % des AS actifs à la fin de l'année 2015 verraient l'ensemble de leurs préfixes propagé dans l'Internet. Cette proportion est comparable à la valeur observée en 2014. Par ailleurs, en

cas de filtrage des annonces invalides uniquement, l'ensemble de l'espace d'adressage géré par un unique AS n'aurait plus été joignable au cours du mois de décembre.

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. Par exemple, ces données n'apportent pas d'information quant à l'utilisation des ROA à des fins de filtrage. Cependant, une étude de l'évolution de la cohérence des déclarations par rapport aux annonces réellement effectuées permet d'obtenir des indices quant à la maintenance dans le temps des ROA dans le dépôt du RIPE-NCC.

	Type	janvier	décembre
Nombre d'AS (IPv4)	Aucun ROA utilisé	7	8
	Quelques ROA utilisés	20	33
	Tous les ROA sont utilisés	161	181
Nombre d'AS (IPv6)	Aucun ROA utilisé	6	11
	Quelques ROA utilisés	2	4
	Tous les ROA sont utilisés	58	69

Table 1.2 – Évolution de l'utilisation des ROA

Le tableau 1.2 donne les résultats de l'étude de l'usage potentiel des déclarations effectuées par les AS français dans la RPKI. En IPv4 comme en IPv6, on remarque qu'une part importante des AS utilise tous leurs ROA. Cependant, on peut également noter que malgré l'adoption faible et récente de la RPKI, il existe tout de même des AS qui n'utilisent aucun de leurs ROA.

À retenir

À la fin de l'année 2015, le constat général reste le même qu'à l'issue de l'année 2014 : les déclarations effectuées dans la RPKI sont loin d'être exhaustives. Ainsi, environ un tiers de l'espace d'adressage IPv4 n'est pas couvert. Pour le protocole IPv6, la couverture reste très faible.

Chapitre 2

Résilience sous l'angle du protocole DNS

2.1 Introduction

Le système de noms de domaine, géré par le protocole DNS [18, 19], est un système de nommage réparti et hiérarchique dont l'objectif principal est d'associer à une adresse IP un nom lisible par les utilisateurs. Ainsi, le nom `www.afnic.fr` permet de retrouver l'adresse IP `192.134.5.5`. 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.` ». Les noms justes en dessous de la racine, comme `.fr`, sont appelés des noms de premier niveau (TLD [1]).

À chaque niveau 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 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 orga-

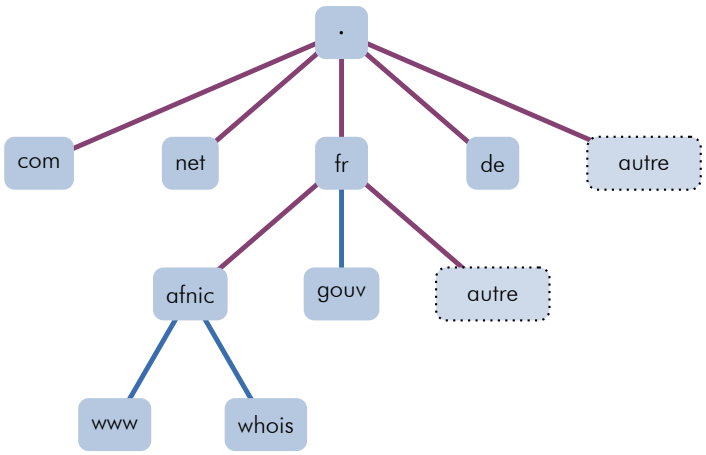


Figure 2.1 – Structure du DNS

1. Top Level Domain.

nisme différent de celui qui administre la zone parente. 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 [2]. Les délégations sont illustrées par des liens violets dans la figure 2.1.

Informations stockées dans le DNS

Les ressources attachées à une zone sont décrites par des enregistrements DNS. Chaque enregistrement 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 et des données qui dépendent du type en question.

Les différents types d'enregistrement DNS sont publiés et maintenus par l'IANA [3] dans un registre dédié aux paramètres du DNS [20]. 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 entrant ;
- `NS` : le nom d'un serveur DNS ;
- `Delegation Signer` et `DNSKEY` : des informations cryptographiques utiles pour DNSSEC [4].

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 [5], interroge l'arborescence DNS en partant de la racine (interaction 2) et en suivant de proche en proche les points de délégation jusqu'au serveur 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 le serveur récursif, et ils lui retournent la réponse ; soit ils l'aiguillent

2. Internet Corporation for Assigned Names and Numbers.
3. Internet Assigned Numbers Authority.
4. Domain Name System Security Extensions.
5. Fournisseur d'Accès à l'Internet.

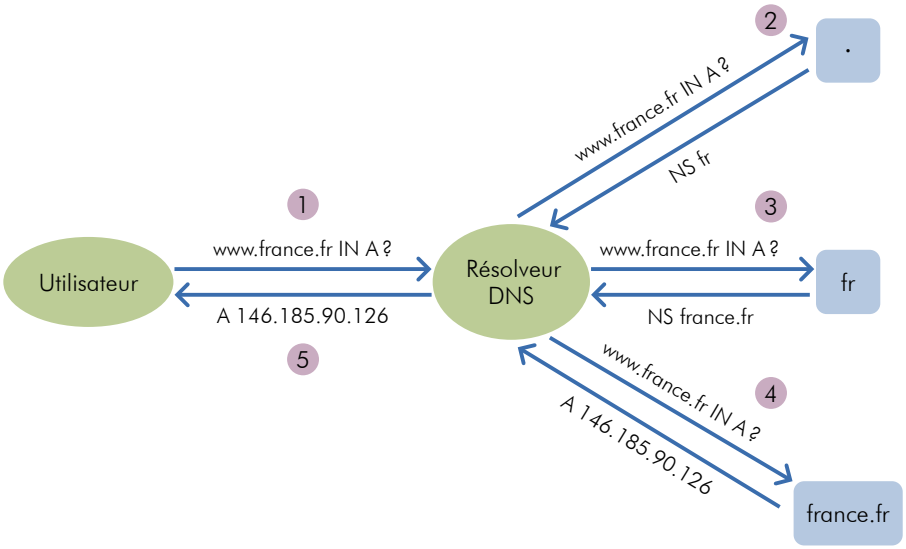


Figure 2.2 – Exemple de résolution DNS

vers d'autres serveurs à interroger qui seraient plus susceptibles de faire autorité pour le nom de domaine recherché.

Juridiction technique des noms de domaine

Les enregistrements DNS de type NS et MX contiennent des noms de serveur, comme illustré dans la figure 2.3. Le nom à gauche du type de l'enregistrement, ici `ssi.gouv.fr`, est l'emplacement dans l'arbre DNS de cet enregistrement. Le nom à droite du type, comme ici `dns1.ssi.gouv.fr`, est la donnée. Les noms à droite doivent généralement être résolus en adresses IP par un serveur récursif afin de répondre aux attentes d'un utilisateur du DNS.

```
ssi.gouv.fr.      NS    ns6.gandi.net.
ssi.gouv.fr.      NS    dns1.ssi.gouv.fr.
ssi.gouv.fr.      MX    10 smtp.ssi.gouv.fr.
```

Figure 2.3 – Exemples d'enregistrements NS et MX

Dans un enregistrement DNS, lorsque le nom à gauche du type est inclus dans le nom à droite, le nom de droite est dit être dans la « juridiction technique ». Par exemple, `dns1.ssi.gouv.fr` est dans la juridiction technique de `ssi.gouv.fr`. Le serveur renvoyant un tel enregistrement NS ou MX peut alors aussi répondre l'adresse IP correspondant au nom. Parfois, cela est même exigé par le protocole.

À l'inverse, les noms de serveur peuvent être situés dans un domaine tiers. Ils sont alors en-dehors de la juridiction technique. C'est le cas de l'enregistrement NS utilisant `ns6.gandi.net` pour déléguer le nom de domaine `ssi.gouv.fr` dans la figure 2.3.

Les noms hors juridiction technique peuvent introduire une dépendance au bon fonctionnement d'un domaine tiers. En effet, chacun constitue un point de défaillance unique, ou SPOF [6], si son dysfonctionnement peut causer l'impossibilité de résoudre un nom en adresse IP. La notion de degrés de dépendance quantifie le nombre de SPOF. Certains tiers sont indispensables et sont donc exclus de ce compte. Il s'agit notamment des zones parentes d'un nom, comme, par exemple, la racine ou `.fr` pour le nom `france.fr`.

Ainsi, `ssi.gouv.fr` aurait un seul degré de dépendance si ce domaine était délégué à un serveur DNS dans le domaine `example.com` et à un autre serveur dans le domaine `example2.com`. En effet, la panne de `example.com` pourrait être compensée par la disponibilité de `example2.com` et inversement. Le seul SPOF serait alors `.com`. De même, `ssi.gouv.fr` aurait un degré de dépendance de deux, s'il était uniquement délégué avec des noms de serveur faisant partie du domaine `example.com`. En effet, le bon fonctionnement des serveurs de deux acteurs serait requis : ceux de `.com` et ceux de `example.com`.

Le risque d'un TLD indisponible n'est pas théorique. Par exemple, en décembre 2015, le TLD `.tr` a subi une attaque DDoS [7] pendant trois semaines [21], avec des périodes où l'ensemble de ses serveurs DNS étaient inaccessibles.

Noms de domaine publics

Dans ce rapport, le terme « noms de domaine publics » désigne les noms de domaine délégués depuis un des domaines définis dans une liste, appelée PSL [8] [22]. Celle-ci provient d'une initiative de Mozilla pour renforcer le cloisonnement logique des sites web dans les navigateurs. Cette liste, bien que n'ayant pas un rapport direct avec le DNS, permet de référencer les domaines gérés par des entités se comportant comme des registres. Cette information n'est pas systématiquement visible dans le DNS. En effet, certains registres n'opèrent pas toujours des noms de domaine composés d'une seule étiquette. C'est le cas notamment du registre Nominet, responsable de `.co.uk`.

Sécurité des enregistrements

Conçu à une époque où la menace était moins forte, le DNS ne bénéficiait pas de mécanismes de sécurité avancés lors de sa création. Le protocole DNSSEC vise à remédier à ce manque [23]. 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 est établie et maintenue grâce à des enregistrements

6. Single Point of Failure.
7. Distributed Denial of Service.
8. Public Suffix List.

DS. Ce mécanisme empêche notamment les attaques dites de « pollution de cache » visant à injecter des enregistrements frauduleux dans un serveur cache.

2.1.1 Données et outils

L'observatoire utilise des scripts *ad hoc* permettant de réaliser des mesures actives des zones DNS. La bibliothèque `dnspython` [24] est notamment utilisée à cette fin.

Les serveurs faisant autorité sur les zones déléguées de `.fr` sont directement interrogés par les scripts. Lorsque plusieurs serveurs faisant autorité existent pour un même nom de domaine, le serveur interrogé est choisi aléatoirement, afin de limiter la charge imposée par la campagne de mesures. La distribution sur laquelle est effectué le tirage aléatoire n'est cependant pas uniforme. Les serveurs ont une probabilité d'être sélectionnés qui est inversement proportionnelle au nombre de zones étudiées qu'ils hébergent.

En résumé, plus un serveur héberge de zones, plus sa probabilité d'être choisi pour résoudre un domaine est faible. S'il retourne une erreur, ou s'il ne répond pas dans le délai imparti, les scripts opèrent une action de repli. Ils ont alors recours à un serveur récursif qui applique son algorithme de résolution habituel.

Les noms de domaine n'ayant pas répondu à nos requêtes ne sont pas comptés dans les statistiques. Ils constituent un biais statistique de près de 3 % des noms de domaine délégués de la zone `.fr` en décembre 2015, soit environ 77 500 noms de domaine. En décembre 2014, ce biais était de 2,5 %, soit 66 000 noms de domaine.

Données utilisées

Les mesures actives ont été réalisées en utilisant la zone `.fr` qui varie au gré des créations, suppressions et modifications de zones déléguées. Lors de l'analyse, seules les zones pour lesquelles l'ensemble des mesures ont pu être conduites sans échec, sont comptabilisées. Elles sont appelées les « zones étudiées ». Ainsi, de 2014 à 2015, le nombre de ces zones a augmenté de 7 % pour atteindre environ 2 810 000 au 7 décembre 2015, contre environ 2 630 000 au 31 décembre 2014. Cette évolution est due à la création de 617 000 nouvelles zones, à la suppression de 438 000 zones et à l'augmentation du nombre de zones en échec lors des mesures.

Le choix d'employer la zone `.fr` comme source de données introduit des biais vis-à-vis de la représentativité de l'Internet français. En effet, l'enregistrement de noms de domaine dans la zone `.fr` n'est pas limité aux seules personnes enregistrées sur le territoire français. Par ailleurs, d'autres TLD existent en France, parmi lesquels les noms géographiques, comme `.re`, ou des noms génériques, comme `.paris`. Finalement, dans le marché des noms de domaine en France, l'usage de TLD étrangers est souvent fait, avec par exemple `.com` ou `.net`.

Il importe de noter que les données utilisées font autorité. Cela signifie que les enregis-

trements DNS utilisés sont directement récupérés auprès des serveurs faisant autorité sur les zones considérées. Ainsi, les enregistrements DS utilisés pour l'indicateur DNSSEC sont extraits de la zone `.fr`, tandis que les enregistrements NS, MX, A, et AAAA sont résolus conformément à la méthode décrite page 33.

La liste des suffixes publics utilisée dans le présent rapport a été téléchargée le 2 décembre 2015 [22]. La notion de noms de second niveau, employée dans le rapport 2014, est remplacée par celle des noms de domaine publics.

Les dates de création des zones étudiées sont obtenues par l'analyse des données publiques de l'Afnic, publiée dans le cadre de l'initiative Opendata [25].

2.2 Dispersion des serveurs DNS faisant autorité

Nombre de serveurs par zone déléguée

Le nombre d'enregistrements NS par zone étudiée est resté globalement équivalent à celui rapporté en 2014. Ainsi, autour de 70 % des zones sont hébergées sur deux serveurs, contre trois serveurs pour environ 18 % des zones. Les fluctuations mineures observées s'expliquent principalement par la dynamique du marché et la création de nouveaux noms hébergés sur des plateformes de service comportant plus ou moins de serveurs DNS.

Le nombre d'enregistrements NS par zone déléguée reste suffisant pour permettre une bonne résilience, du point de vue de cet indicateur. En effet, moins de 1 % des zones n'utilisent qu'un seul enregistrement NS, qui pourrait donc constituer un SPOF.

La même étude peut être effectuée, une fois les noms de serveurs contenus dans les enregistrements NS résolus. En IPv4 comme en IPv6, la répartition est sensiblement équivalente à celle observée en ne tenant compte que des enregistrements NS. En conséquence, pour les zones étudiées, employer plusieurs adresses IP de la même version du protocole IP, pour un même enregistrement NS, peut être considéré comme une pratique anecdotique.

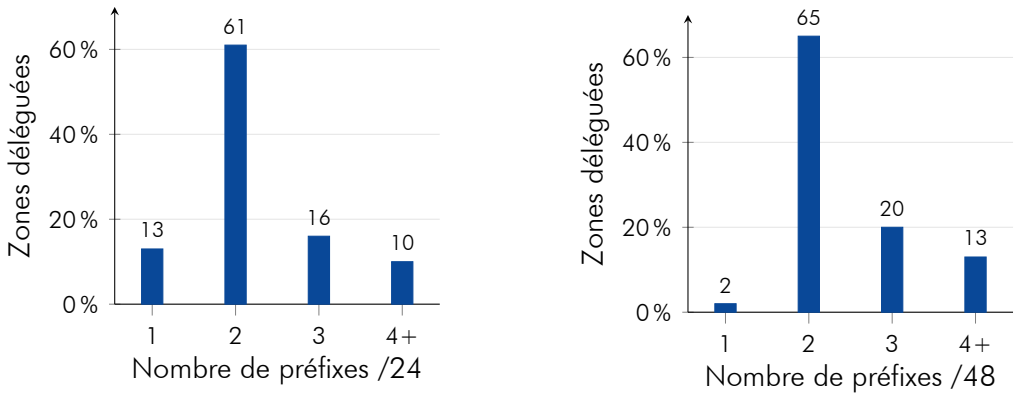
Il convient néanmoins de constater que près de 41 % des zones ne disposent d'aucun serveur ayant une adresse IPv6. Les zones dans ce cas de figure reposent exclusivement sur la disponibilité des serveurs en IPv4, même si les serveurs récursifs les interrogeant disposaient simultanément d'une connectivité IPv4 et IPv6. Cette proportion observée en 2015 est équivalente à celle rapportée par l'observatoire en 2014.

À retenir

Le nombre de serveurs DNS par zone semble suffisant pour assurer une bonne résilience. Le déploiement d'IPv6 sur les serveurs DNS faisant autorité a stagné en 2015. Ainsi, environ 41 % des zones ne sont accessibles qu'en IPv4.

Dispersion topologique des zones déléguées

La dispersion topologique des serveurs DNS est une exigence issue de l'ingénierie de la résilience [26, 27]. La dispersion des serveurs de noms dans des AS distincts peut, dans certains cas, contribuer à éviter des indisponibilités en cas d'incident ayant un impact sur la totalité du réseau d'un opérateur. En 2015, le nombre moyen d'AS par zone reste équivalent à celui de 2014, et stagne à 1,2. Par ailleurs, la quantité de



(a) En IPv4

(b) En IPv6

Figure 2.4 – Dispersion des zones par nombre de préfixes en décembre 2015

zones hébergées par un seul AS reste stable depuis 2011, culminant à 83 % des zones étudiées.

La dispersion des serveurs DNS dans des AS différents reste donc très faible. Il est pour autant difficile de tirer, à partir de ce constat, une conclusion directe sur l'impact potentiel en disponibilité. Une analyse plus fine des réseaux des opérateurs serait nécessaire afin d'estimer la vraisemblance d'un incident unique affectant l'intégralité de leur réseau.

À retenir

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

Répartir, ou être en mesure de répartir, ses serveurs de noms dans des préfixes /24 en IPv4 et /48 en IPv6 distincts peut également constituer une bonne pratique de résilience[9]. Cela permet notamment de limiter les zones de pollution BGP et d'accroître l'agilité face aux dénis de service distribués.

L'étude de la répartition des serveurs de noms dans des préfixes est effectuée uniquement sur les zones étant hébergées sur au moins deux adresses IP. En IPv4, la figure 2.4a montre que 87 % des zones peuvent être ou sont annoncées dans des préfixes /24 distincts. En IPv6, ce chiffre s'élève à 98 % pour des préfixes /48 distincts, comme détaillé dans la figure 2.4b.

9. Les tailles de préfixes /24 en IPv4 [28] et /48 en IPv6 [29] sont les plus longues pouvant être annoncées sur Internet, selon les bonnes pratiques BGP actuellement admises.

À retenir

Les bonnes pratiques de résilience vis-à-vis de la diversité des préfixes et de la résistance aux usurpations BGP sont mises en œuvre pour pratiquement la totalité des zones étudiées.

Dispersion géographique des serveurs DNS faisant autorité

La dispersion géographique des serveurs DNS faisant autorité peut également avoir un impact sur la disponibilité des services de l'Internet français. Par exemple, cela peut être le cas suite à la rupture de câbles sous-marins isolant les utilisateurs d'un service des serveurs DNS renseignant l'adresse IP à contacter.

En utilisant la base GeoLite de Maxmind [30], téléchargée en décembre 2015, il est possible d'estimer la géolocalisation des serveurs faisant autorité sur les zones étudiées. Cette pratique présente néanmoins un intérêt limité si la technique de routage *anycast*, présentée dans le rapport 2013, est employée. En effet, dans ce cas, l'IP géolocalisée dans un pays sera annoncée avec BGP depuis plusieurs endroits dans le monde. Ce sous-indicateur permet néanmoins d'obtenir une première approximation de l'emplacement de ces serveurs.

Comme pour les années précédentes, en 2015, tant en IPv4 qu'en IPv6, près de 82 % des zones étudiées sont servies exclusivement par des serveurs faisant autorité situés dans un même pays.

En IPv4, les zones dont tous les serveurs DNS faisant autorité sont dans un même pays étranger représentent 27 % des zones étudiées. Il convient néanmoins de noter que 75 % d'entre elles sont hébergées dans un pays ayant une frontière terrestre avec la France métropolitaine. Cette situation ne présente donc, a priori, pas un risque significatif. Pour près de 20 % de ces zones, le constat est plus mitigé, ces dernières étant hébergées en Amérique du Nord.

Pour IPv6, les zones hébergées dans un seul pays étranger représentent 30 % des zones ayant des serveurs DNS accessibles en IPv6. Parmi celles-ci, près de 85 % sont hébergées dans un pays ayant une frontière terrestre avec la France métropolitaine.

À retenir

La dispersion géographique des zones étudiées est globalement satisfaisante, tant en IPv4 qu'en IPv6. Néanmoins, près de 20 % des zones sont servies en IPv4, exclusivement depuis l'Amérique du Nord.

Dépendance à des noms tiers

L'analyse des enregistrements NS révèle que 99 % des zones sont déléguées en utilisant exclusivement des noms de serveur hors juridiction technique.

Le risque d'indisponibilité causé par les degrés de dépendance n'est pas qu'un risque théorique. Par exemple, en 2015, le site `tools.ietf.org` a été indisponible pendant plusieurs heures. Tous les serveurs DNS faisant autorité sur cette zone étaient désignés par des noms de serveur dans le domaine tiers `levkowetz.com`. Lorsque ce domaine tiers a subi un incident en disponibilité, `tools.ietf.org` est devenu inaccessible à son tour.

Les données de l'observatoire indiquent que 89 % des zones déléguées étudiées ont au moins un degré de dépendance : tous les enregistrements NS utilisent un nom situé dans un même TLD distinct de `.fr`, comme par exemple `.net`.

De même, 75 % des zones étudiées ont deux degrés de dépendance, dûs à l'usage d'un seul nom de domaine public hors juridiction et situé dans un TLD tiers, à l'instar de `tools.ietf.org` qui était dépendant de `levkowetz.com`.

À retenir

Pour 75 % des zones étudiées, il existe un risque d'indisponibilité accru du fait des noms de serveur choisis pour déléguer ces zones.

2.3 Mise en œuvre de DNSSEC

Analyse des enregistrements DS

Pour ce rapport, le dénombrement des enregistrements DS [10] s'effectue à partir des données contenues dans la zone `.fr`, après un filtrage pour ne conserver que les zones pour lesquelles les mesures pour le reste du rapport ont été menées sans échec. Cette nouvelle méthodologie devrait permettre d'améliorer la reproductibilité des résultats en n'utilisant que des informations publiques. Les années précédentes, certains enregistrements DS correspondaient, en effet, à des tests, ou à des zones non publiées par l'Afnic.

L'évolution du nombre de zones disposant d'au moins un enregistrement DS selon la nouvelle méthodologie a été observée en utilisant les zones étudiées du 14 décembre 2014 et du 6 décembre 2015.

Avec ces nouvelles données, entre décembre 2014 et décembre 2015, le pourcentage de zones étudiées ayant des enregistrements DS a évolué de 6,4 % à 8,8 %. Pour simplifier, le terme *zone DNSSEC* est utilisé pour désigner de telles zones. En décembre 2015, il était ainsi possible de dénombrer environ 248 000 zones dans ce cas de figure, contre 180 000 en décembre 2014.

Afin de déterminer l'origine de cette évolution, il est intéressant de détailler la croissance de la zone `.fr`. Ainsi, 617 000 zones ont été créées entre décembre 2014 et décembre 2015. Cela représente 22 % des zones étudiées fin 2015. De plus, pendant la même période, environ 438 000 zones ont été supprimées, soit 16 % des zones étudiées en décembre 2014. Parmi ces 438 000 zones, 173 000 avaient été créées pour une durée d'un an et n'ont pas renouvelées.

Comparativement, le nombre de zones mettant en œuvre DNSSEC est composé d'environ 98 000 zones nouvellement enregistrées, soit 40 % des zones DNSSEC en décembre 2015. De plus, environ 54 000 zones ont été supprimées de la zone `.fr`, soit 30 % des zones DNSSEC en décembre 2014. Parmi les 54 000 zones ainsi supprimées, environ 36 000 avaient été créées en 2014.

En plus de la dynamique de croissance des zones DNSSEC, il est intéressant de souligner qu'environ 29 000 zones déjà enregistrées en 2014 ont mis en œuvre DNSSEC en 2015. Par ailleurs, environ 6000 zones signées en 2014 ont désactivé DNSSEC au cours de l'année. Ces zones représentent 3 % des zones DNSSEC en 2014.

La croissance de DNSSEC est donc essentiellement due aux créations de zones. Ainsi, à peine 1 % des zones étudiées, qui existaient déjà en 2014, ont mis en œuvre DNSSEC au cours de l'année 2015.

10. Delegation Signer.

À retenir

Un peu moins de 9 % des zones étudiées mettent en œuvre DNSSEC en 2015. La croissance est essentiellement due à la création de nouvelles zones en 2015.

Analyse des algorithmes cryptographiques

Près de 92 % des zones étudiées et disposant d'un enregistrement DS indique utiliser la suite cryptographique `RSASHA1-NSEC3-SHA1`. La quasi-totalité des 8 % restants utilise la suite `RSASHA256`. Il convient de constater que l'usage de l'algorithme de hachage SHA-1, tel qu'employé dans la suite cryptographique `RSASHA1-NSEC3-SHA1`, est contraire aux bonnes pratiques actuelles communément admises en cryptographie [31], et aux recommandations du RGS [11] [32].

L'analyse des algorithmes employés pour hacher les clés DNSSEC des zones étudiées contraste avec le résultat précédent. Ainsi, SHA-256 est employé par près de 98 % des zones disposant d'un enregistrement DS afin de créer la chaîne de confiance DNSSEC. Les 2 % restants utilisent SHA-1.

À retenir

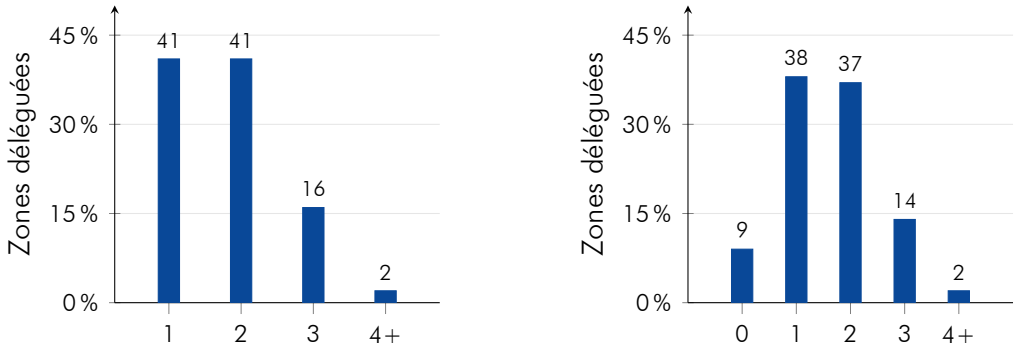
Près de 92 % des zones étudiées mettent en œuvre l'algorithme de hachage SHA-1, jugé insuffisant d'après les bonnes pratiques actuellement admises en cryptographie. À l'inverse, près de 98 % des zones étudiées utilisent bien l'algorithme de hachage recommandé SHA-256 pour créer la chaîne de confiance DNSSEC.

11. Référentiel Général de Sécurité.

2.4 Dispersion des relais de messagerie entrants

Nombre de relais par zone déléguée

L'observatoire a modifié sa méthodologie concernant cet indicateur. En 2014, les pourcentages étaient calculés par rapport au nombre de zones ayant au moins un enregistrement MX. Certaines zones ne disposent néanmoins pas d'un relais de messagerie entrant, ce qui produisait un biais statistique. En 2015, environ 9 % des zones étudiées n'ont aucun enregistrement MX.



(a) Ancienne méthodologie

(b) Nouvelle méthodologie

Figure 2.5 – Nombre de relais de messagerie entrants par domaine en 2015

En 2015, les zones étudiées présentent un faible nombre de relais de messagerie entrants, en moyenne. Ainsi, un seul relais est disponible pour 38 % des zones étudiées, comme l'indique la figure 2.5b. En cas d'incident, la défaillance de ce relais unique provoque alors une indisponibilité totale du service. Si elle reste de courte durée, l'impact est cependant limité. Le protocole de livraison de courriers électroniques (SMTP) est, en effet, lui-même conçu de façon résiliente.

Les chiffres de 2014 ne sont pas exprimés dans la figure 2.5, puisqu'ils sont identiques à ceux de 2015.

À retenir

Un seul relais de messagerie est renseigné pour 38 % des zones déléguées. Le risque d'impossibilité de recevoir de nouveaux messages électroniques est donc accru par la présence d'un SPOF.

Un unique enregistrement MX ne signale pour autant pas la présence d'un SPOF au niveau du plan d'adressage. En effet, plusieurs adresses IP peuvent être indiquées pour

un même nom de domaine ou une IP peut être annoncée sur l'Internet en employant la technique de l'anycast. De même, une adresse IP peut être virtuelle et répartie sur plusieurs serveurs physiques, grâce à des répartiteurs de charge.

Ainsi, seul le cas où plusieurs adresses IP sont associées à un nom peut être analysé au travers du DNS. Pour cela, les noms de domaine indiqués dans les enregistrements MX ont été résolus en adresses IPv4 et IPv6.

Le nombre d'adresses IPv4 s'avère généralement identique au nombre d'enregistrements MX. Il existe néanmoins un cas particulier concernant près de 14 % des zones. Ces zones sont partiellement ou totalement hébergées sur une certaine plateforme de service. Elle met à disposition un relais de messagerie secondaire [12] désigné par un seul enregistrement MX. Le nom de serveur contenu dans cet enregistrement MX est résolu en cinq adresses IPv4 distinctes. Les zones employant ce service bénéficient donc d'une plus grande résilience, puisqu'elles disposent d'au moins six adresses IPv4 au total.

À retenir

L'analyse des adresses IPv4 des relais de messagerie entrants montre une situation légèrement meilleure qu'en analysant uniquement les noms de serveur des enregistrements MX. Concernant les relais de messagerie, près de 38 % des zones restent néanmoins hébergées sur une seule adresse IPv4.

Par opposition, pour près de 89 % des zones, aucun des noms de serveur contenus dans les enregistrements MX n'a d'adresse IPv6 associée. Parmi les 11 % restants, pour 81 % de ces zones, un seul nom contenu dans les enregistrements MX peut être résolu en une unique IPv6.

Il est intéressant de noter qu'une plateforme de service a un comportement atypique. Cette dernière représente 10 % des zones dont les relais disposent d'adresses IPv6. Lorsque les noms de serveur de cette plateforme sont résolus, une unique adresse IPv6 est retournée. Celle-ci est distincte mais constante en fonction du serveur faisant autorité interrogé. La sélection de l'adresse IPv6 du relais de messagerie est donc dépendante du serveur récursif et de son algorithme de sélection du serveur faisant autorité. L'observatoire a choisi d'agréger toutes les adresses IP retournées comme s'il s'agissait d'un unique jeu d'enregistrements `AAAA`. La taille de ce jeu d'enregistrements varie de 14 à 18 adresses IPv6 par nom de serveur.

12. Un relais secondaire peut notamment stocker les messages en cas d'indisponibilité des serveurs primaires. Les messages sont ensuite envoyés aux serveurs primaires, lorsque ceux-ci sont à nouveau accessibles.

À retenir

IPv6 reste peu déployé. Ainsi, pour près de 89 % des zones, aucun des noms de serveur contenus dans les enregistrements MX n'a d'adresse IPv6 associée. Parmi les 11 % restants, pour 81 % de ces zones, un seul nom contenu dans les enregistrements MX peut être résolu en une unique IPv6.

Analyse des noms de serveur des relais entrants

L'étude des noms de serveur des relais entrants dans les enregistrements `MX` permet de compter leurs degrés de dépendance, selon la méthodologie présentée page 31. Un biais statistique s'était également glissé dans ce sous-indicateur, en 2014. Celui-ci était dû aux pourcentages calculés à partir de la zone complète au lieu de compter uniquement les domaines ayant des enregistrements MX. Les chiffres de 2014 et 2015 sont néanmoins similaires.

En 2015, 86 % des zones étudiées disposent d'un ou plusieurs degrés de dépendance pour leurs relais de messagerie. Les 14 % restants disposent d'au moins un relais de messagerie désigné par un nom dans la juridiction technique.

Environ 1 700 000 zones étudiées utilisent exclusivement des noms de serveur situés dans un autre TLD que `.fr`. Pour 99 % de ces zones, un degré de dépendance est introduit puisque tous les relais sont désignés par des noms sous un unique TLD. Pour 69 % d'entre elles, ce TLD est `.net` et pour 23 %, ce TLD est `.com`. Ces deux TLD sont sous la responsabilité d'un même organisme américain et sont hébergés sur le même ensemble de serveurs DNS [33].

Un degré de dépendance est également introduit pour les 19 % de zones utilisant des noms de serveur – relais de messagerie – dans un unique domaine hors juridiction mais délégué sous `.fr`. Enfin, 64 % des zones étudiées sont affligées de deux degrés de dépendance, puisque leurs relais sont désignés exclusivement avec des noms situés dans un unique nom public situé dans un TLD tiers.

À retenir

Jusqu'à 86 % des zones étudiées introduisent au moins un SPOF dû au choix des noms de leurs relais de messagerie. En particulier, 64 % des zones étudiées créent deux SPOF en utilisant des noms situés dans un nom public situé sous un unique TLD tiers.

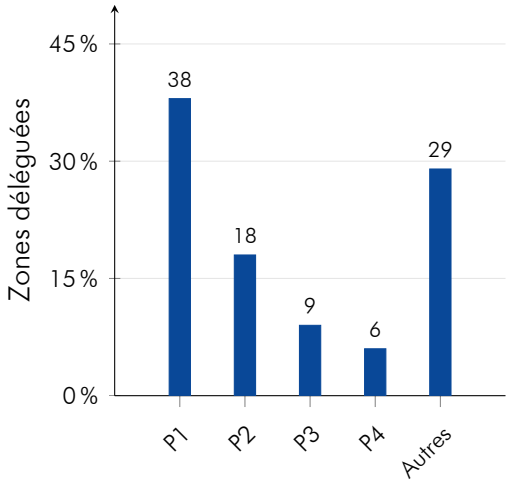


Figure 2.6 – Concentration des relais de messagerie sur des plateformes, en 2015

Concentration des relais de messagerie entrants

L'analyse des noms publics permet également de mesurer la concentration des relais de messagerie sur quelques plateformes d'hébergement mutualisé.

Pour les résultats suivants, seule l'étiquette la plus à gauche du nom public est considérée, sans tenir compte du nom du registre. Il est ainsi possible de regrouper certaines plateformes qui sont diversifiées sur plusieurs registres ou TLD. Par exemple, des relais de messagerie situés dans des sous-domaines de `1and1.com` et `1and1.co.uk` seront considérés comme hébergés par `1and1`. Afin de mieux considérer les risques, seules les zones dont tous les relais sont hébergés par une unique plateforme sont comptées. Cet ensemble est constitué d'environ 1 800 000 zones.

Comme le montre la figure 2.6, une très forte concentration des relais de messagerie s'opère sur une poignée de plateformes d'hébergement. En particulier, 71 % des relais de messagerie sont hébergés par quatre opérateurs.

Cette concentration peut parfois aider à la mutualisation des moyens. Cela peut présenter un intérêt pour la défense contre certaines attaques en déni de service. Le filtrage du courrier indésirable peut également être partagé. Il convient de noter, néanmoins, un risque de défaillance collective en cas d'incident affectant les composants mis en commun.

Dispersion des relais de messagerie par pays

La répartition des relais de messagerie dans plusieurs pays, à l'instar des serveurs DNS, peut être un facteur affectant la disponibilité. En particulier, assurer la connectivité avec les utilisateurs susceptibles d'envoyer des courriers électroniques est souhaitable.

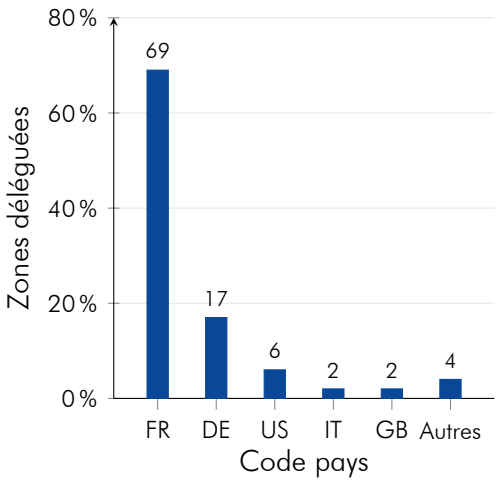


Figure 2.7 – Géolocalisation des relais hébergés dans un seul pays, en IPv4, en 2015

En IPv4, concernant les zones étudiées et disposant d'enregistrements MX, 99 % d'entre elles utilisent des relais de messagerie tous situés dans un même pays. Cela représente donc environ 2 540 000 zones. En IPv4, 69 % de ces zones ont leurs relais localisés en France. Comme l'illustre la figure 2.7, le seul pays hors de l'Europe et contenant un nombre significatif de relais de messagerie est les États-Unis d'Amérique, avec 6 % des zones concernées.

En IPv6, il convient de rappeler que près de 89 % des zones ne disposent d'aucun relais de messagerie en IPv6. Seules 248 000 zones sont donc concernées par cette étude. Ainsi, 85 % de ces zones utilisent des relais de messagerie tous situés dans un même pays. Pour 221 000 zones, ce pays est la France. La quasi-totalité des zones restantes est située en Europe.

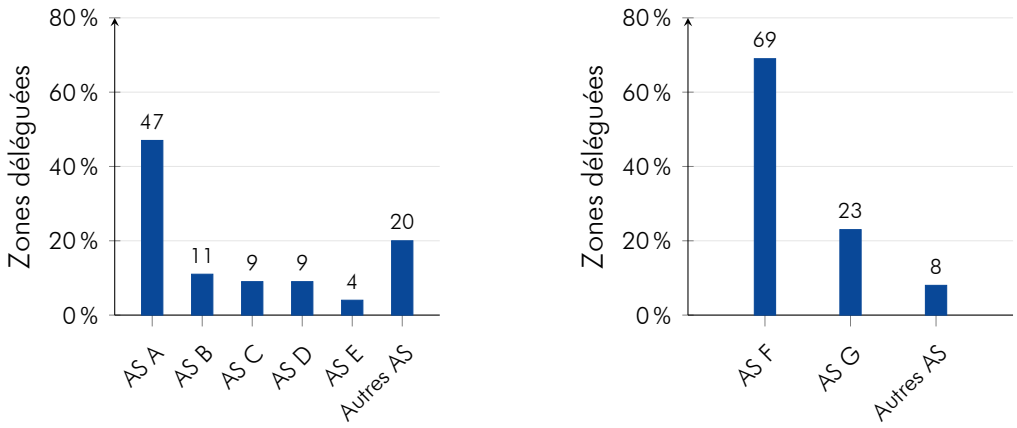
À retenir

L'essentiel des relais de messagerie des zones étudiées est localisé en France, tant en IPv4 qu'en IPv6.

Dispersion réseau des relais de messagerie

Ce sous-indicateur étudie la répartition des relais de messagerie sur un ou plusieurs opérateurs identifiés par leur numéro d'AS.

En IPv4, dans 96 % des cas, tous les relais de messagerie d'une zone sont hébergés dans un seul AS. Le reste des zones a ses relais hébergés quasi intégralement dans deux AS. En IPv6, les nombres sont comparables, avec 98 % des zones dont tous les relais



(a) En IPv4 (b) En IPv6

Figure 2.8 – Répartition par AS des relais hébergés dans un seul pays, en 2015

sont au sein d'un même AS. Ces nombres révèlent une faible diversité des opérateurs hébergeurs. Ce constat corrobore celui dressé par le sous-indicateur employant les noms de domaines publics, présenté à la page 44.

En analysant le nombre de relais de messagerie par numéro d'AS, il est possible de dresser un portrait de cette concentration, du point de vue du routage. Ainsi, en IPv4, 47 % des relais de messagerie sont concentrés au sein d'un unique AS. Par ailleurs, quatre opérateurs hébergeurs regroupent à eux seuls 80 % des relais de messagerie des zones étudiées. Cette répartition est illustrée par la figure 2.8a. En IPv6, la concentration est encore plus forte, puisque 69 % des relais sont hébergés par un même acteur. Le deuxième acteur en héberge quant à lui 23 %, comme le montre la figure 2.8b.

À retenir

La concentration des relais de messagerie entrants sur quelques opérateurs réseaux est significative. En IPv4, un opérateur est responsable de la connectivité de 47 % des relais des zones étudiées. En IPv6, ce chiffre monte à 69 %.

Chapitre 3

Résilience sous l'angle du protocole TLS

3.1 Introduction

3.1.1 Fonctionnement du protocole TLS

La mise en place d'une session TLS entre un client et un serveur permet d'assurer l'intégrité et la confidentialité des communications, indépendamment de la nature des applications sous-jacentes. Parmi les utilisations les plus courantes du protocole figure HTTPS, qui consiste en la protection des flux HTTP à l'intérieur de tunnels TLS.

Le développement du protocole TLS a suivi plusieurs itérations [34, 35, 36] depuis la conception du protocole SSL [1], désormais obsolète [37]. Par souci d'interopérabilité, les spécifications permettent aux deux parties impliquées de négocier la version du protocole qu'ils adopteront communément.

Ce paramètre est établi au cours d'une phase *TLS handshake* qui précède le chiffrement effectif des échanges. De même, les spécifications autorisent l'utilisation de différentes combinaisons d'algorithmes cryptographiques ; la suite cryptographique [2] retenue pour la session étant déterminée grâce aux messages de type `handshake`.

Sans se substituer aux références plus précises [38, 39], la figure 3.1 illustre la négociation de ces paramètres dans un cas générique à l'aide d'interactions numérotées :

1. le client initie une requête en envoyant un message de type `ClientHello`, contenant notamment les suites cryptographiques qu'il prend en charge ;
2. le serveur répond par un `ServerHello` qui contient la suite retenue ;
3. le serveur envoie un message `Certificate`, qui contient en particulier sa clé publique au sein d'un certificat numérique ;
4. le serveur transmet dans un `ServerKeyExchange` une valeur éphémère qu'il signe à l'aide de la clé privée associée à la clé publique précédente ;
5. le serveur manifeste sa mise en attente avec un `ServerHelloDone` ;
6. après vérification du certificat et authentification de la valeur précédente, le client choisit à son tour une valeur éphémère qu'il chiffre à l'aide de la clé publique du certificat puis transmet dans un `ClientKeyExchange` ;

1. Secure Sockets Layer.
2. En anglais, *ciphersuite*.

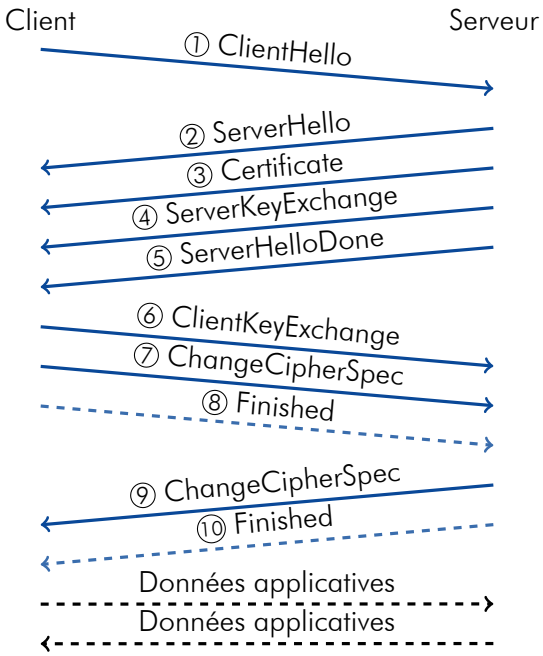


Figure 3.1 – Initiation générique d'une session TLS

7. le client signale l'adoption de la suite négociée avec un `ChangeCipherSpec` ;
8. le client envoie un `Finished`, premier message protégé selon la suite cryptographique avec les secrets issus de l'échange de clés éphémères précédent ;
9. le serveur signale l'adoption de la même suite avec un `ChangeCipherSpec` ;
10. le serveur envoie à son tour un `Finished`, son premier message sécurisé.

Le cas générique décrit ici sous-entend l'adoption d'une des suites cryptographiques qui assurent la propriété de confidentialité persistante, ou PFS [3]. Celle-ci consiste à prévenir le déchiffrement de messages de sessions passées quand bien même la clé privée du serveur serait compromise, en négociant un secret éphémère à l'aide d'un échange Diffie–Hellman [40].

Les spécifications du protocole définissent par ailleurs plusieurs messages supplémentaires et extensions qui permettent d'encadrer et d'enrichir la protection des communications [41]. Un `ClientHello` peut par exemple contenir une extension précisant les capacités de cryptographie sur courbes elliptiques du client.

3.1.2 Les infrastructures de gestion de clés

La validité du certificat envoyé par le serveur au cours de l'initiation de la session TLS est au cœur de la sécurité du protocole. L'ensemble des mécanismes et des entités qui

3. Perfect Forward Secrecy.

formulent cette validité et la maintiennent représente une IGC.

Pour un certificat conforme à la norme X.509 [42] suivie dans le cadre de TLS, l'assurance que la clé publique qu'il contient appartienne effectivement au serveur qu'il annonce en tant que sujet (généralement sous la forme d'un nom de domaine) repose sur la transmission de confiance depuis une autorité déjà reconnue jusqu'au serveur en question. Les liens de confiance successifs établis par des AC [4] sont matérialisés par des signatures cryptographiques apposées aux différents certificats.

Ainsi, le message `Certificate` dont est extraite la clé à l'origine des secrets de session contient en réalité une chaîne de certificats, dont le client attend qu'elle forme un lien depuis une racine de confiance jusqu'au serveur interrogé. Dans le cas de navigateurs web, ces racines correspondent généralement à un registre public, tel que le magasin de certificats NSS maintenu par Mozilla pour son navigateur Firefox [43]. Certaines applications interagissent directement avec le registre public concerné pour mettre à jour leur magasin de certificats de confiance, tandis que d'autres s'appuient sur la maintenance opérée par le système d'exploitation hôte.

Les certificats contiennent plusieurs attributs, tels qu'une clé publique et une période de validité, qui sont habituellement complétés par des extensions X.509v3. Celles-ci permettent notamment de préciser le cadre d'utilisation du certificat en question et de renforcer les assurances de l'IGC. L'ANSSI recommande à cet effet le suivi de l'annexe A4 du RGS [44].

3.1.3 Données et outils

Les mesures de l'observatoire se sont concentrées sur les ressources web accessibles à travers l'Internet français. Elles concernent plus spécifiquement les ressources exposées via le port 443, traditionnellement alloué par les serveurs aux échanges HTTPS. Les enjeux liés aux ressources de messagerie en ligne diffèrent en plusieurs points [45] et ne sont pas abordés dans le présent rapport.

Les noms de domaine issus du registre maintenu par l'Afnic [5] ont été préfixés de `www.` avant d'être résolus. Par exemple, les mesures effectuées sur le domaine `afnic.fr` correspondent à l'adresse IPv4 résolue pour `www.afnic.fr`. Lorsque le port 443 du serveur interrogé était ouvert, l'observatoire a envoyé différents stimulus `ClientHello`, dont les variations visaient à évaluer plusieurs capacités du serveur, telles que sa prise en charge de la confidentialité persistante ou encore sa tolérance envers des versions obsolètes du protocole.

Les réponses obtenues ont été disséquées et insérées en base de données à l'aide de Parsifal [46]. L'outil utilisé était par ailleurs en mesure de vérifier, et éventuellement

4. Autorités de Certification.
5. Association Française pour le Nommage Internet en Coopération.

reconstruire, les chaînes de certificats observées. L'examen plus précis de certains certificats tirait parti de la prise en charge de X.509 par Scapy [47].

L'extension SNI[6] [41] n'ayant pas été utilisée au sein des `ClientHello`, les mesures ne réunissent pas l'ensemble des ressources exposées via HTTPS sur la zone `.fr`. En interrogeant de ce fait un serveur par nom de domaine résolu, un sous-ensemble de 61 216 serveurs accessibles a ainsi été interrogé en juillet 2015, contre 26 261 en février 2014.

6. Server Name Indication.

3.2 Négociation de sessions

Parmi les paramètres de session initialement définis par les spécifications, certains sont reconnus d'usage sûr en 2015, tandis que d'autres ont été déclarés obsolètes car sujets à des attaques [48, 37]. Les attributs établis via la phase de négociation ont donc un impact direct sur la sécurité des échanges subséquents. Pour cette raison, l'observatoire a cherché à établir un profil des serveurs de la zone `.fr` exposant des ressources HTTPS.

Dans la mesure où, soumis aux `ClientHello` appropriés, un même serveur peut par exemple accepter la version recommandée TLS 1.2 mais aussi les versions proscrites SSLv2 et SSLv3, l'examen d'un seul paramètre ne permet pas de juger la sécurité d'un ensemble de serveurs de façon absolue. La mise en commun de ces paramètres et le suivi de leur évolution de 2014 à 2015 permettent cependant un constat qualitatif du respect des bonnes pratiques.

État général des serveurs TLS

En 2015, considérant l'ensemble des stimuli tentant de négocier une session TLS 1.2 ou TLS 1.0, avec des variations notamment au niveau des suites cryptographiques proposées, 80 % des serveurs présentant un port 443 ouvert permettaient d'initier une session TLS. Seuls 3,5 % des serveurs n'envoyaient aucune donnée quel que soit le stimulus utilisé, et 0,4 % répondaient des données jamais reconnues en tant que messages TLS.

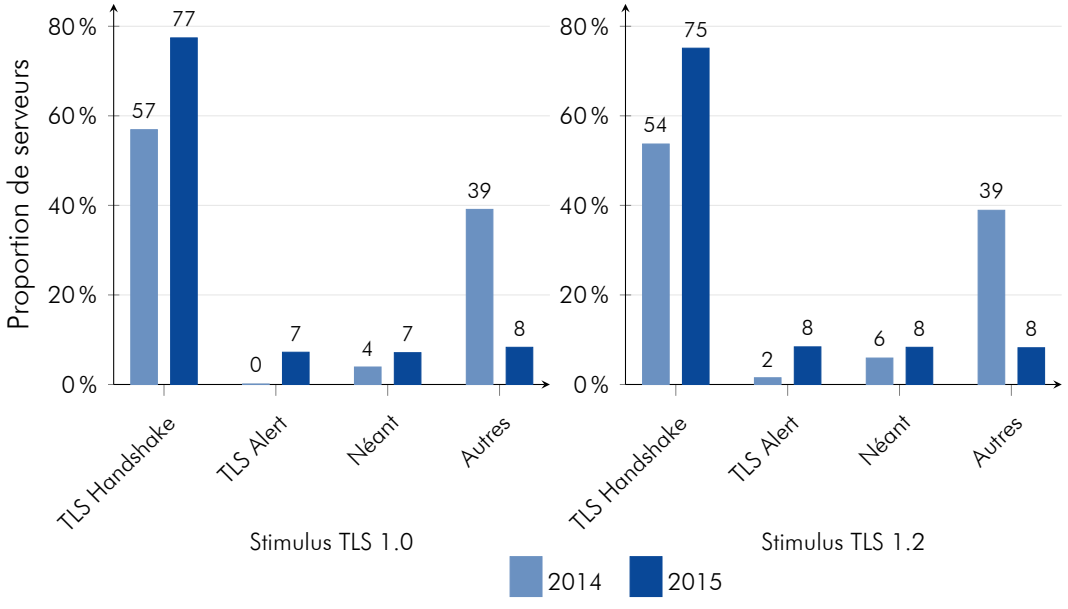


Figure 3.2 – Évolution des réponses des serveurs HTTPS aux stimuli TLS 1.0 et 1.2

La figure 3.2 précise les taux de succès d'établissement de session lors de la campagne de mesure principale avec TLS 1.2 en 2014 puis en 2015, dont le stimulus proposait plusieurs suites cryptographiques sans contrainte particulière. 75 % des serveurs sont aptes à négocier une session TLS 1.2, en nette augmentation par rapport aux 54 % de 2014. La proportion de messages non reconnus est passée de 39 % à 8 % ; un examen manuel révèle plusieurs profils de réponse, notamment des pages HTML non chiffrées et des entêtes SSH.

Lors de la campagne principale menée pour TLS 1.0, le stimulus utilisé permettait encore la négociation d'un nombre varié de suites. Les résultats obtenus sont aussi représentés sur la figure 3.2. Les proportions et leurs évolutions sont semblables à celles observées avec la campagne précédente. Ainsi, l'adoption de la version 1.2 n'est pas pour autant synonyme d'une disparition de la version 1.0. Bien que la version 1.2 prémunisse les communications de certaines attaques qui peuvent affecter la version 1.0 [49], les serveurs maintiennent en général l'interopérabilité avec des clients datés.

À retenir

TLS 1.2 est couramment pris en charge par les serveurs de la zone `.fr` en 2015. TLS 1.0 est présent à égale mesure, mais clients comme serveurs devraient privilégier la version la plus récente du protocole.

Confidentialité persistante

La réalisation des échanges DHE [7] et ECDHE [8] est conditionnée par le choix d'une suite cryptographique appropriée. Le respect de la confidentialité persistante peut donc être mesuré en dénombrant les serveurs qui acceptent l'utilisation de telles suites.

Différentes mesures ont été agrégées afin d'identifier les serveurs proposant la confidentialité persistante. La figure 3.3 illustre la proportion d'adresses IP distinctes où des suites avec DHE ou ECDHE ont pu être négociées, par rapport à l'ensemble des adresses où un port 443 ouvert a été observé. Mi-2015, près de trois quarts des serveurs offraient la confidentialité persistante, en progression depuis début 2014.

Cette tendance positive doit toutefois être tempérée par le fait que la tolérance à DHE ou ECDHE ne garantisse pas qu'un échange de clé éphémère soit préféré en toutes circonstances. De plus, pour des raisons d'interopérabilité, il reste rare que cette protection soit exigée par un serveur.

7. Diffie–Hellman Ephemeral.
8. Elliptic Curve Diffie–Hellman Ephemeral.

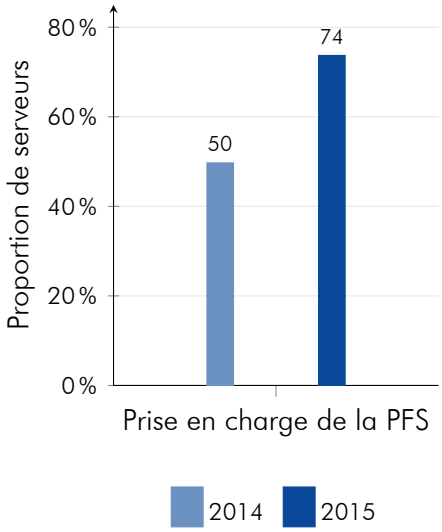


Figure 3.3 – Évolution de la prise en charge de la PFS par les serveurs HTTPS

À retenir

En 2015, l'offre de confidentialité persistante s'est généralisée sur la zone `.fr`. Les serveurs doivent privilégier cette méthode auprès des clients qui la prennent en charge.

Obsolescence de SSLv2

Depuis sa publication initiale par Netscape en 1995, la sécurité de SSLv2 a fait l'objet de critiques qui ont motivé la définition de SSLv3 un an plus tard et, ultimement, une déclaration formelle d'obsolescence en 2011 par l'IETF [48]. En 2015, SSLv2 est désactivé par défaut dans les navigateurs web récents, tandis que sa dangerosité continue d'être évaluée à la hausse [50].

La figure 3.4 représente les réponses des serveurs de la zone `.fr` ayant reçu un `ClientHello` SSLv2. Le message est ignoré par 75 % des serveurs début 2014, et par 78 % des serveurs en 2015. Bien qu'il existe un code erreur permettant de rejeter les versions de protocole non prises en charge, seuls 3 % des serveurs répondaient avec un message de type `alert` en 2015.

Moins d'un serveur sur cinq accepte de monter une session SSLv2, bien que la diminution par rapport à 2014 reste faible. Par ailleurs, ajusté au nombre plus important de serveurs en 2015, l'évolution indique qu'au moins 5000 nouveaux serveurs acceptant SSLv2 ont été configurés entre les deux mesures, malgré sa dangerosité reconnue.

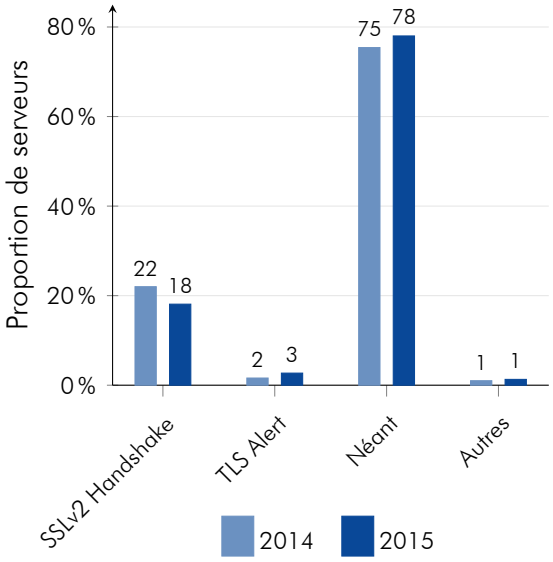


Figure 3.4 – Réponses des serveurs français à un stimulus SSLv2

L'observatoire n'a pas réalisé de mesures relatives à la prise en charge de SSLv3. L'utilisation de cette version est pareillement à proscrire, comme l'ont encore confirmé de récentes études [51].

À retenir

En 2015, de nombreux serveurs tolérant SSLv2 sont apparus. Cette version de protocole doit être abandonnée au plus vite.

3.3 Robustesse des signatures de certificats

L'emploi d'algorithmes de signature robustes pour la construction de chaînes de certificats est essentiel pour la sécurité des échanges avec les serveurs impliqués dans l'IGC. Ces algorithmes combinent généralement une méthode de chiffrement asymétrique avec une fonction de hachage, telle que SHA-2 ou SHA-1. Cependant, plusieurs attaques théoriques contre SHA-1 ont été mises au jour depuis 2005 [52, 53], poussant notamment les éditeurs de navigateurs web à planifier l'obsolescence de cette fonction dans le cadre des IGC.

Ainsi, en 2015, la plupart des navigateurs détectant l'utilisation de SHA-1 émettaient un avertissement à l'attention de l'internaute [54]. Depuis début 2016, les certificats signés à l'aide de SHA-1 et valides au plus tôt le 1er janvier 2016 sont rejetés. Le rejet de l'ensemble des certificats signés à l'aide de SHA-1, initialement prévu pour le 1er janvier 2017, pourrait être avancé au début de l'été 2016 [55, 56, 57].

Évolution de l'ensemble des certificats

Ces considérations autour de la résistance du paradigme de confiance ont motivé l'observatoire à étudier le profil des certificats observables sur la zone `.fr`. Du fait que l'extension SNI n'ait pas été utilisée, les mesures ont relevé au plus un certificat terminal par nom de domaine résolu et par stimulus, et ne sont donc pas exhaustives. Elles permettent toutefois de caractériser des tendances significatives.

Certificats	février 2014	juillet 2015
Auto-signés	5324	15 712
Délivrés par une AC	7554	22 759

Table 3.1 – Nombre de certificats distincts observés sur la zone `.fr`

Le tableau 3.1 fait état du nombre de certificats distincts relevés au cours des deux campagnes de mesure lancées sur la zone `.fr` en 2014 puis 2015. À près de dix-huit mois d'écart, la proportion de certificats auto-signés de 41 % est restée inchangée. Sur les 15 712 représentants observés en 2015, 47 étaient reconnus en tant que racines de confiance par le magasin de certificats NSS.

La confiance accordée à un certificat auto-signé est arbitraire et ne repose pas sur sa signature. La qualité d'une IGC est par conséquent indépendante des algorithmes de signature utilisés pour ses racines de confiance. Pour cette raison, la figure 3.5 représente l'évolution de la présence des différents algorithmes de hachage de 2014 à 2015 en faisant abstraction des certificats auto-signés, qu'ils soient reconnus ou non par des magasins de confiance publics.

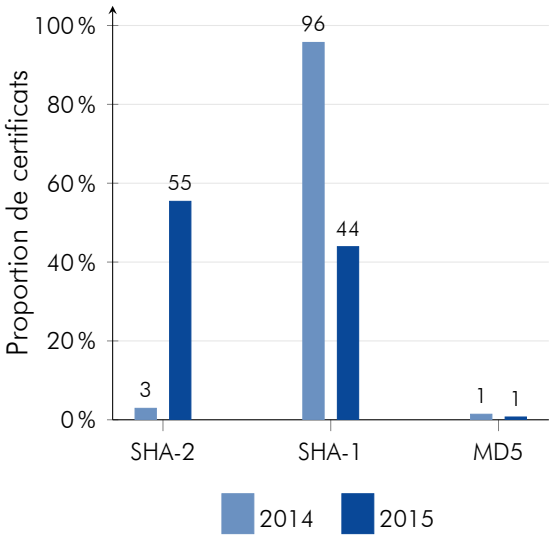


Figure 3.5 – Évolution des signatures des certificats

Début 2014, la part de certificats signée à l'aide de SHA-2 était de 3 % seulement, tandis que 96 % d'entre eux étaient signés avec SHA-1. Le résidu de 1 % utilisait MD5, un algorithme a priori dangereux pour une IGC car vulnérable à des attaques par collision [58].

Mi-2015, le taux de présence de SHA-2 est monté à 55 %, et le taux de présence de SHA-1 est descendu en conséquence à 44 %. L'annonce du rejet progressif de SHA-1 s'est ainsi nettement retranscrite en une adoption positive de SHA-2, bien qu'une proportion conséquente de certificats signés à l'aide de SHA-1 demeure encore en usage. SHA-256 est, à 98 %, la fonction la plus répandue de la famille SHA-2.

Un résidu de 1 % de certificats signés avec MD5 demeure. Un examen manuel des adresses IP concernées montre qu'il s'agit essentiellement de serveurs non utilisés, renvoyant des pages HTML vides ou laissées par défaut. L'impact de cette persistance de MD5 serait donc minime.

Apparition de nouveaux certificats

Parmi les certificats précédemment observés, certains ont été signés plusieurs années avant les mesures. Pour cette raison, l'analyse globale des certificats de la zone `.fr` ne reflète que partiellement l'évolution des pratiques d'émission de la part des autorités de certification. C'est en observant le profil des certificats les plus récents que ces dernières pourront être établies.

Cependant, en dehors de l'initiative *Certificate Transparency* en cours de standardisation [59], il n'existe pas de registre public faisant état des dates d'émission des certificats X.509. La date d'émission peut différer de celle du début de la période de validité, mais

aussi de celle de la première apparition publique. Conscient de l'approximation effectuée, l'observatoire a isolé les certificats observés en juillet 2015 et valides depuis le 1er janvier 2015 au plus tôt.

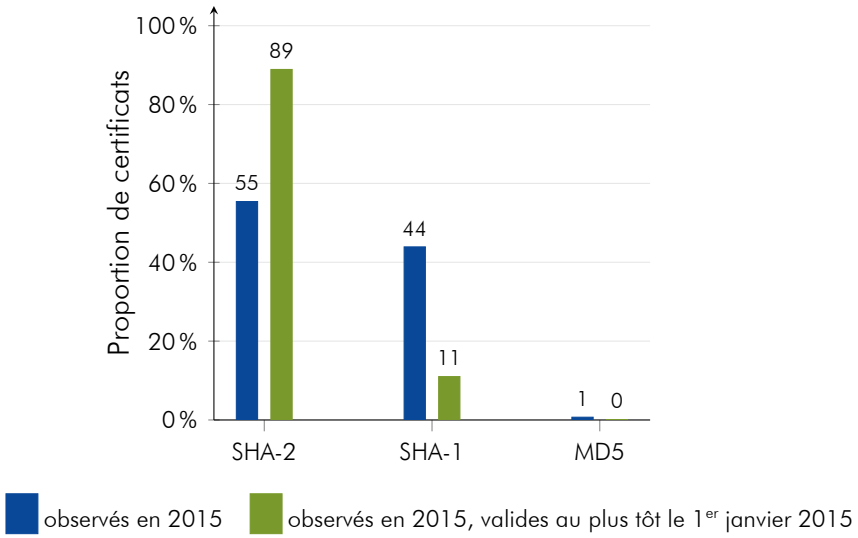


Figure 3.6 – Évolution des signatures dans l'émission de nouveaux certificats

La comparaison entre les 22 759 certificats non auto-signés relevés en juillet 2015 et le sous-ensemble des 9475 certificats valides depuis le 1er janvier 2015 au plus tôt est illustrée par la figure 3.6. Pour les nouveaux certificats, les taux d'utilisation de SHA-2, et SHA-1 sont respectivement de 89 % et 11 %, caractérisant une transition manifeste vers SHA-2. Par ailleurs, seuls 10 certificats signés avec MD5 ont été observés.

À retenir

En juillet 2015, plus de la moitié des certificats de la zone `.fr` étaient signés à l'aide de l'algorithme SHA-2. Conformément aux bonnes pratiques, les certificats récemment émis ne reposent presque plus sur SHA-1.

Conclusion générale

Parmi les différentes améliorations apportées aux méthodologies de l'observatoire, les analyses offrent une nouvelle vision de l'Internet français. Il est désormais possible d'appréhender les paramètres ayant un impact sur la sécurité des échanges effectués en HTTPS. Ainsi, la version recommandée TLS 1.2 est prise en charge par 75 % des serveurs de zones déléguées sous `.fr`. De même, une grande partie d'entre eux offrent une confidentialité persistante (PFS) à leurs utilisateurs.
Par ailleurs, vis-à-vis de la robustesse des certificats, l'observatoire a mis en évidence la quasi-disparition des signatures effectuées avec SHA-1 au profit de SHA-2. En juillet 2015, plus de la moitié des certificats étaient signés, conformément aux bonnes pratiques, avec SHA-2. Il s'agit d'un résultat particulièrement encourageant concernant l'étude du protocole TLS qui confirme la pertinence d'observer et de comparer l'évolution d'un protocole à l'aide d'indicateurs techniques stables.

Concernant le protocole IPv6, les tendances amorcées les années précédentes se confirment en 2015. Sous l'angle de BGP, le nombre d'AS français mettant en œuvre IPv6 a augmenté de 13 % au cours de l'année contre 6 % en 2014, pour finir à environ 300 en fin d'année. La situation est cependant moins satisfaisante sur d'autres aspects. Ainsi, l'adoption d'IPv6 pour les serveurs DNS et les serveurs de messagerie est stagnante, et a peu évolué entre 2014 et 2015. Contrairement aux années précédentes, le nombre de préfixes non couverts par des objets `route6` augmente. La couverture reste aussi très faible avec la RPKI : plus de 99 % de l'espace d'adressage IPv6 n'est pas couvert par les `ROA`. Sans être alarmantes, ces différentes observations semblent indiquer des changements dans la mise en œuvre du protocole IPv6.

Parmi les observations effectuées en 2015, certaines apparaissent comme problématiques. Ainsi, la dispersion des relais de courriers électroniques entrants reste faible en IPv4, et inquiétante en IPv6. De même, ces relais sont fortement concentrés sur un nombre réduit de plateformes de services, ce qui pourrait nuire à leur disponibilité. Pour les serveurs de noms, les bonnes pratiques de résilience et de dispersion sont mises en œuvre. Cependant les dépendances des noms de domaines en dehors de `.fr` introduisent des risques supplémentaires.
D'autre part, l'observatoire a noté un ralentissement de l'adoption du protocole DNSSEC, et l'utilisation massive de l'algorithme de hachage `SHA-1`, jugé insuffisant d'après les bonnes pratiques en cryptographie actuellement admises. Il semble ainsi nécessaire d'amorcer rapidement la transition à un algorithme plus robuste comme `SHA-256`. Finalement, vis-à-vis du protocole TLS, l'observatoire déplore les résultats concernant SSLv2. Ainsi, entre 2014 et 2015, près de 5000 nouveaux serveurs ont été configurés

avec ce protocole, malgré sa dangerosité reconnue.

Au regard des analyses concernant l'année 2015, l'observatoire renouvelle ses encouragements aux acteurs de l'Internet concernant l'appropriation des bonnes pratiques d'ingénierie admises pour les protocoles BGP [3], DNS [4], et TLS. L'observatoire les encourage également à anticiper la menace que représentent les DDoS [5]. En ce qui concerne le protocole IPv6, 2015 semble être une année charnière. Malgré, l'augmentation du nombre d'AS français mettant en œuvre IPv6, les bonnes pratiques d'exploitation de ce protocole, étudiées dans ce rapport, semblent peu suivies. D'autre part, l'observatoire énonce les recommandations suivantes :

- **surveiller les annonces de préfixes** et se tenir prêt à réagir aux usurpations ;
- **utiliser des algorithmes supportant la confidentialité persistante**, et **abandonner SSLv2 et SHA-1** au profit de mécanismes plus robustes ;
- **diversifier le nombre de serveurs SMTP et DNS** afin d'améliorer la robustesse de l'infrastructure ;
- **appliquer les bonnes pratiques** notamment celles rappelées dans ce document, 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, "MaBo - MRT and BGP in OCaml." <https://github.com/ANSSI-FR/mabo>.

[2] ANSSI, "TaBi - Track BGP Hijacks." <https://github.com/ANSSI-FR/tabi>.

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

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

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

[6] Vivet, Nicolas and Valadon, Guillaume, "Tools to Detect Routing Anomalies," tech. rep., May 2016.

[7] 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, 7606, 7607, 7705.

[8] M. Lepinski, Ed., "BGPSEC Protocol Specification - draft-ietf-sidr-bgpsec-protocol-15." <http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-15>, 2016.

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

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

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

[12] RIPE-NCC, "Dépôt RPKI." <rsync://rpki.ripe.net/>.

[13] Spotify, "Luigi - Build complex pipelines of batch jobs." <https://github.com/spotify/luigi>.

[14] "Disco MapReduce," tech. rep.

[15] BGPMON, "Large scale bgp hijack out of india." <http://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/>, November 2015.

[16] BGPMON, "Bgp optimizer causes thousands of fake routes." <http://www.bgpmon.net/bgp-optimizer-causes-thousands-of-fake-routes/>, May 2015.

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

[18] 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.

[19] 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, 7766.

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

[21] Attila Özgit, ".tr DDoS Attack." <https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ddos-07mar16-en.pdf>, Dec. 2015.

[22] "Public Suffix List." <https://publicsuffix.org/>.

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

[24] Bob Halley, "DNSPython Library." <http://www.dnspython.org/>.

[25] Afnic, "Opendata .fr." <https://opendata.afnic.fr/fr/produits-et-services/le-fr/opendata-fr.html>.

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

[27] R. Bush, D. Karrenberg, M. Kosters, and R. Plzak, "Root Name Server Operational Requirements." RFC 2870 (Best Current Practice), June 2000. Obsoleted by RFC 7720.

[28] RIPE-NCC, "RIPE Routing Working Group Recommendations on Route Aggregation." <http://www.ripe.net/ripe/docs/ripe-399>, Dec. 2006.

[29] RIPE-NCC, "RIPE Routing Working Group Recommendations on IPv6 Route Aggregation." <http://www.ripe.net/ripe/docs/ripe-532>, Nov. 2011.

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

[31] Damien Giry, "Cryptographic Key Length Recommendation." <http://www.keylength.com/fr>, Sept. 2015.

[32] ANSSI, "Référentiel Général de Sécurité," tech. rep., June 2014.

[33] ICANN, "Root zone." https://www.internic.net/domain/root.zone.

[34] T. Dierks and C. Allen, "The TLS Protocol Version 1.0." RFC 2246 (Proposed Standard), Jan. 1999. Obsoleted by RFC 4346, updated by RFCs 3546, 5746, 6176, 7465, 7507.

[35] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1." RFC 4346 (Proposed Standard), Apr. 2006. Obsoleted by RFC 5246, updated by RFCs 4366, 4680, 4681, 5746, 6176, 7465, 7507.

[36] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2." RFC 5246 (Proposed Standard), Aug. 2008. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685.

[37] R. Barnes, M. Thomson, A. Pironti, and A. Langley, "Deprecating Secure Sockets Layer Version 3.0." RFC 7568 (Proposed Standard), June 2015.

[38] O. Levillain, "SSL/TLS, 3 ans plus tard." <http://www.ssi.gouv.fr/uploads/2015/06/SSTIC2015-Article-ssltls_soa_reloaded-levillain_cObDbqp.pdf>, Juin 2015.

[39] I. Ristić in *Bulletproof SSL and TLS*, Feisty Duck, August 2014.

[40] E. Rescorla, "Diffie-Hellman Key Agreement Method." RFC 2631 (Proposed Standard), June 1999.

[41] D. E. 3rd, "Transport Layer Security (TLS) Extensions : Extension Definitions." RFC 6066 (Proposed Standard), Jan. 2011.

[42] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280 (Proposed Standard), May 2008. Updated by RFC 6818.

[43] Mozilla, "Network security services." <https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS>.

[44] Agence nationale de la sécurité des systèmes d'information (ANSSI), "Référentiel Général de Sécurité - Annexe A4." <https://references.modernisation.gouv.fr/sites/default/files/RGS_v-2-0_A4.pdf>.

[45] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. A. Halderman, "Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security," in *Internet Measurement Conference (IMC)*, October 2015.

[46] "Parsifal : an OCaml-based parsing engine." <https://github.com/ANSSI-FR/parsifal>.

[47] "Scapy : the Python-based interactive packet manipulation program & library." <https://github.com/secdev/scapy>.

[48] S. Turner and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0." RFC 6176 (Proposed Standard), Mar. 2011.

[49] J. Rizzo and T. Duong, "Browser Exploit Against SSL/TLS." <https://packetstormsecurity.com/files/105499/Browser-Exploit-Against-SSL-TLS.html>, October 2011.

[50] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, and Y. Shavitt, "DROWN : Breaking TLS using SSLv2." <https://drownattack.com/drown-attack-paper.pdf>, March 2016.

[51] B. Möller, T. Duong, and K. Kotowicz, "This POODLE bites : Exploiting the SSL 3.0 Fallback," tech. rep., September 2014.

[52] H. Y. Xiaoyun Wang, "Advances in cryptology – crypto 2005 : 25th annual international cryptology conference, santa barbara, california, usa, august 14-18, 2005. proceedings," 2005.

[53] M. Stevens, P. Karpman, and T. Peyrin, "Freestart collision for full SHA-1." <https://eprint.iacr.org/2015/967>, 2016.

[54] Google, "Gradually sunsetting SHA-1." <https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html>, September 2014.

[55] Microsoft, "SHA-1 Deprecation Update." <https://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update/>, November 2015.

[56] Google, "An update on SHA-1 certificates in Chrome." <https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html>, November 2015.

[57] Mozilla, "Continuing to Phase Out SHA-1 Certificates." <https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/>, December 2015.

[58] H. Y. Xiaoyun Wang, "How to break md5 and other hash functions," in *EUROCRYPT'05*, pp. 19–35, 2005.

[59] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency." RFC 6962 (Experimental), June 2013.

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
DHE	Diffie–Hellman Ephemeral
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DS	Delegation Signer
ECDHE	Elliptic Curve Diffie–Hellman Ephemeral
FAI	Fournisseur d'Accès à l'Internet
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
PFS	Perfect Forward Secrecy
PSL	Public Suffix List
RGS	Référentiel Général de Sécurité
RIPE-NCC	RIPE Network Coordination Centre
RIR	Regional Internet Registry
RIS	Routing Information Service

ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure
SNI	Server Name Indication
SPOF	Single Point of Failure
SSL	Secure Sockets Layer
TLD	Top Level Domain
TLS	Transport Layer Security

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 2016

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