Résilience de l'Internet français

2016

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

Document réalisé par l'ANSSI.

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 et de l'Afnic pour leur contribution, 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.

ANSSI-OBS-2016 v1.0 Document validé le 13 juillet 2017.

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

rapport.observatoire@ssi.gouv.fr

Table des matières

Synthèse 5

Présentation de l'observatoire 7

Introduction 9

1 Résilience sous l'angle du protocole BGP 11

1.1 Introduction 11

1.2 Connectivité des AS français 15

1.3 Usurpations de préfixes 20

1.4 Utilisation des objets route 24

1.5 Déclarations dans la RPKI 26

2 Résilience sous l'angle du protocole DNS 29

2.1 Introduction 29

2.2 Dispersion des serveurs DNS faisant autorité 34

2.3 Mise en œuvre de DNSSEC 38

2.4 Dispersion des relais de messagerie entrants 40

3 Résilience sous l'angle du protocole TLS 47

3.1 Introduction 47

3.2 Négociation de sessions 51

3.3 Robustesse des signatures de certificats 54

4 Étude des sources de DDoS en France 57

Conclusion générale 63

Bibliographie 65

Acronymes 71

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.

Rédigé par l'ANSSI, ce rapport étudie la résilience de l'infrastructure de l'Internet à travers les protocoles BGP et DNS. Le premier protocole permet d'échanger des données grâce aux annonces de routage, tandis que le second permet de traduire un nom de domaine, pour un site web par exemple, en des informations techniques. Par ailleurs, l'observatoire étudie depuis deux ans le service de chiffrement des communications utilisé par les navigateurs web : TLS. L'actualité autour des attaques DDoS a encouragé le recensement et le signalement d'équipements en France pouvant être utilisés pour participer à des attaques de type DDoS.

En 2016, trois faits marquant se dégagent. Le premier concerne la signature de certificats HTTPS par SHA-1 qui a quasiment disparu grâce à la forte implication des éditeurs de navigateur web. Le second concerne IPv6, où l'observatoire déplore le fait que la situation ne s'améliore pas, les bonnes pratiques d'exploitation de ce protocole continuant d'être peu suivies. Enfin, près de 92 % des zones DNSSEC utilisent l'algorithme obsolète SHA-1 pour les signer.

L'observatoire encourage l'ensemble des acteurs de l'Internet à s'approprier les bonnes pratiques d'ingénierie admises pour les protocoles BGP [1], DNS [2], et TLS [3], et à anticiper la menace que représentent les DDoS [4]. Aussi, l'observatoire énonce les recommandations suivantes :

- **surveiller les annonces de préfixes** et se tenir prêt à réagir aux usurpations ;
- **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 ;
- **anticiper les attaques DDoS** en acquérant une solution de dépollution ou souscrire à une offre via un prestataire.

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[1] 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 des bonnes pratiques admises.

1. Agence nationale de la sécurité des systèmes d'information.

Introduction

Depuis 2011, l'observatoire rédige un rapport faisant un état des lieux de l'Internet en France. Les objectifs étaient, dans un premier lieu, d'améliorer la connaissance du fonctionnement de l'Internet, mais aussi d'y intégrer de manière active les différents acteurs du marché. Chaque occurence de ce rapport réalise une étude par l'intermédiaire d'indicateurs techniques utilisant des données publiques. L'objectif étant de prodiguer des recommandations pragmatiques à destination des acteurs de l'Internet.

Les premiers indicateurs définis reposent sur les protocoles BGP et DNS, nécessaires au fonctionnement de la structure de l'Internet. Le premier permet aux différents acteurs de s'interconnecter entre eux, mais aussi d'échanger et d'acheminer le trafic Internet. Le second permet de faire la correspondance entre un nom de domaine et une adresse IP. L'observatoire s'est ensuite intéressé aux services via l'analyse de la messagerie électronique, et des sites web mettant en œuvre HTTPS grâce à TLS. Cette année, l'actualité a motivé l'ajout d'un indicateur relatif aux vecteurs d'attaques de type DDoS.

Une partie des attaques DDoS utilisent le mécanisme de réflexion, qui consiste à générer du trafic à destination d'un service ouvert sur Internet en positionnant comme adresse IP source celle de la victime. Dès lors, le service ouvert répond à la victime. Ces attaques utilisent aussi le principe d'amplification en visant des services pour lesquels une petite requête génère une réponse de très grande taille. L'ANSSI recense depuis 2015 les services ouverts sur l'Internet en France pouvant servir de vecteurs à ces attaques, et signale aux responsables de ces adresses IP qu'ils hébergent des services pouvant être exploités par des attaquants. Les attaques DDoS sont l'affaire de tous et seule une coordination entre les acteurs peut permettre d'en diminuer l'impact.

Les recommandations ont amené l'équipe de l'observatoire, avec la participation des acteurs du marché en France, à rédiger des guides pour l'accompagnement dans la configuration des interconnexions BGP [1], l'acquisition et administration de noms de domaines [2], comprendre et anticiper les attaques DDoS [4]. Enfin, pour permettre à la communauté d'aller plus loin, l'observatoire a publié des outils tels que mabo [5] et tabi [6] qui facilitent l'analyse des données BGP.

À retenir

Les opérateurs désireux d'obtenir des informations détaillées concernant les indicateurs BGP, mais aussi les adresses IP de leur réseau pouvant servir de vecteur pour des attaques DDoS, peuvent solliciter des rapports individualisés.

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 [2] [7]. L'objectif de ce protocole est d'échanger des informations de joignabilité de préfixes entre deux opérateurs qui sont alors appelés AS [3] 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*.

1. Internet Protocol.
2. Border Gateway Protocol.
3. Autonomous System.

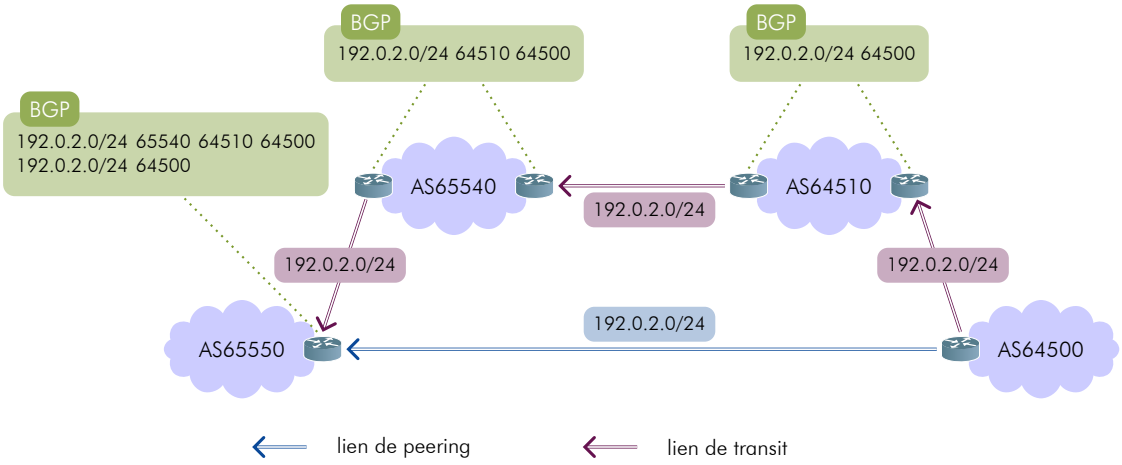

Figure 1.1 – Exemple de chemins d'AS sur des liens de transit et peering

Il n'existe aucune méthode d'authentification robuste des annonces de préfixes. Par conséquent, un AS malveillant peut annoncer un préfixe appartenant à un autre AS. C'est ce que l'on appelle une usurpation de préfixe [4]. 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 entraîner une redirection du trafic destiné au réseau victime vers le réseau ayant usurpé les préfixes.

1.1.2 Les objets route

Les bonnes pratiques [1] veulent qu'un organisme déclare, dans la base `whois`, les préfixes qu'il annonce en BGP. Ces déclarations doivent être effectuées par l'intermédiaire d'objets `route` et sont stockées dans les serveurs d'un IRR [5]. Ce service est opéré par chaque RIR [6], dont le RIPE-NCC [7] 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`

4. En anglais, *hijack*.
5. Internet Routing Registry.
6. Regional Internet Registry.
7. 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 des protections 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 [8] [8], est toujours en cours de conception à l'IETF [9]. 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 [10] [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 [11] dédiée à la certification des ressources IP (préfixes IP ou numéro d'AS) dont il a la gestion. 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 [12] 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.

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

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 [13] [10]. Treize routeurs spécifiques, appelés collecteurs, enregistrent 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 logiciel libre. Ainsi, la transformation des messages binaires BGP dans un format textuel intermédiaire est assurée par l'outil *MaBo* [5]. La détection d'usurpation de préfixes est réalisée par *TaBi* [6] et l'étude de la connectivité des AS par l'outil *AS Rank* [11].

L'industrialisation de ces outils a fait l'objet d'un travail important par l'équipe de l'observatoire, dans le but de produire les indicateurs 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].

1.1.5 Évolution des AS français

En 2016, à l'aide de la méthode définie dans les précédents rapports, l'observatoire a identifié 1649 AS français, dont 1072 ont été vus [14] au moins une fois au cours de l'année dans les archives BGP.

Près de 92 % des AS français visibles l'ont été pendant toute l'année. Parmi les 8 % d'AS visibles restants, près de 40 % d'entre eux ont été actifs pendant au moins un trimestre. Enfin, 577 AS recensés n'ont pas annoncé de préfixes au cours de l'année 2016.

À retenir

En 2016, l'observatoire a identifié 1649 AS français. Parmi ceux-ci, le nombre d'AS actifs, c'est-à-dire annonçant au moins un préfixe, est de 1020 à la fin du mois de décembre 2016, contre 1001, fin décembre 2015.

13. Routing Information Service.
14. Un AS est considéré comme visible s'il a annoncé au moins un préfixe au cours de l'année.

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, deux AS sont reliés par une arête 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 1.4 et 1.5. Il apparaît 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 2016. La figure 1.3 montre ainsi qu'en IPv4, le rythme de croissance est d'environ 6 %. Soit un nombre très proche de celui observé en 2015. En IPv6, il est d'environ 16 %, contre 13 % l'année précédente.

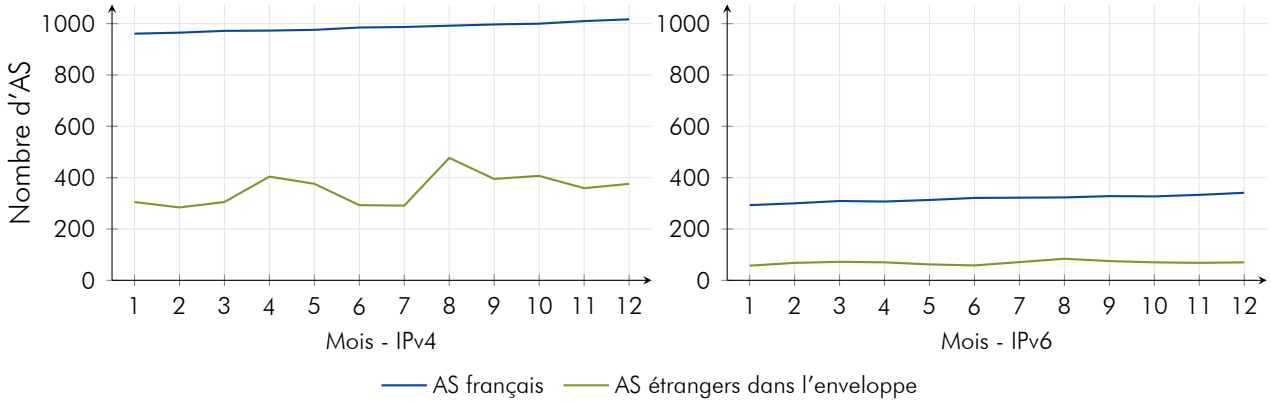

Figure 1.3 – Évolution du nombre d'AS français et de l'enveloppe en 2016

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 1.3 montre qu'en IPv4 leur nombre est d'environ 400, un nombre supérieur à celui observé en 2015. En IPv6, comme entre 2013 et 2015, une cinquantaine d'AS étrangers est nécessaire pour interconnecter tous les AS français.

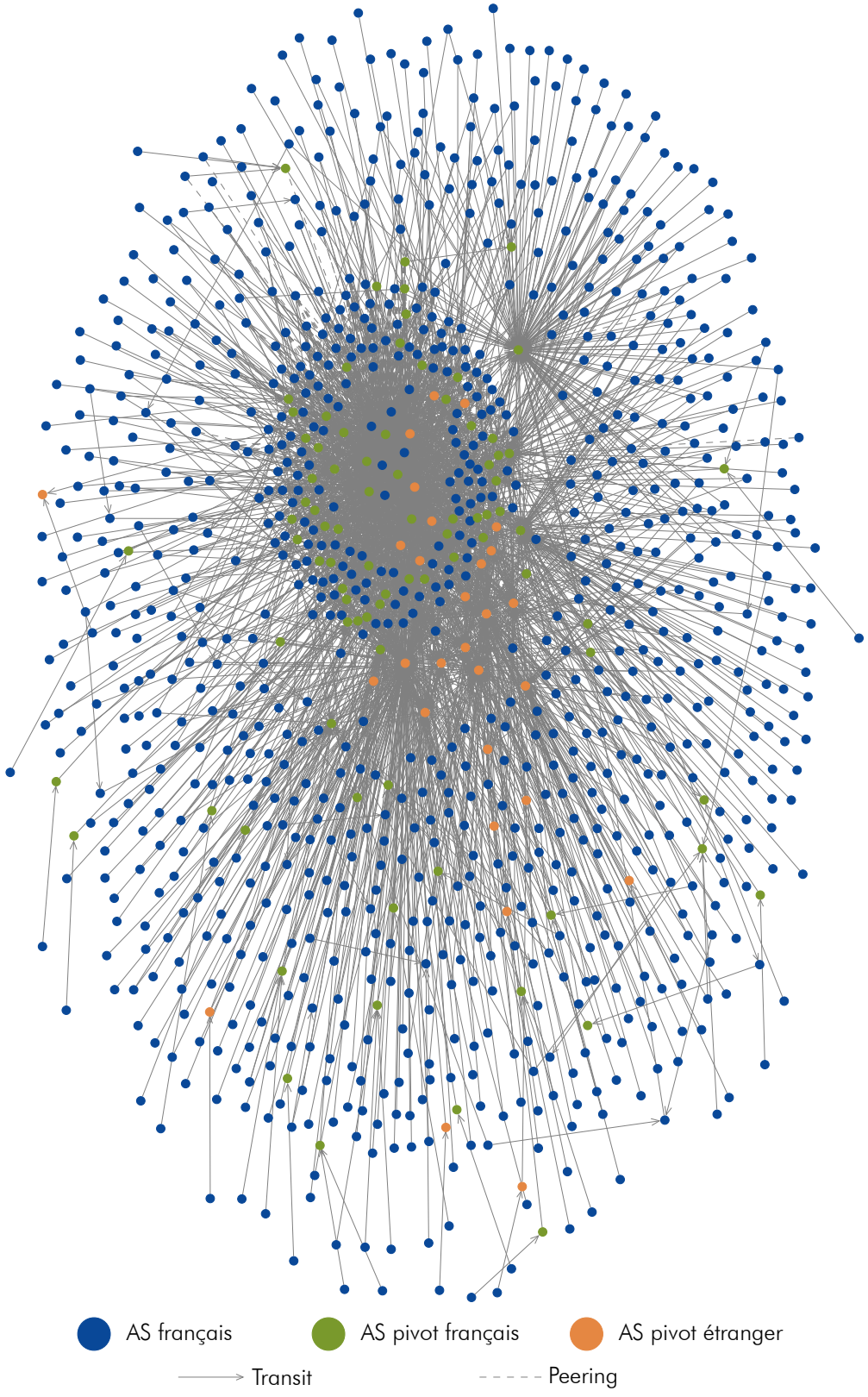

Figure 1.4 – Graphe de connectivité en IPv4 (décembre 2016)

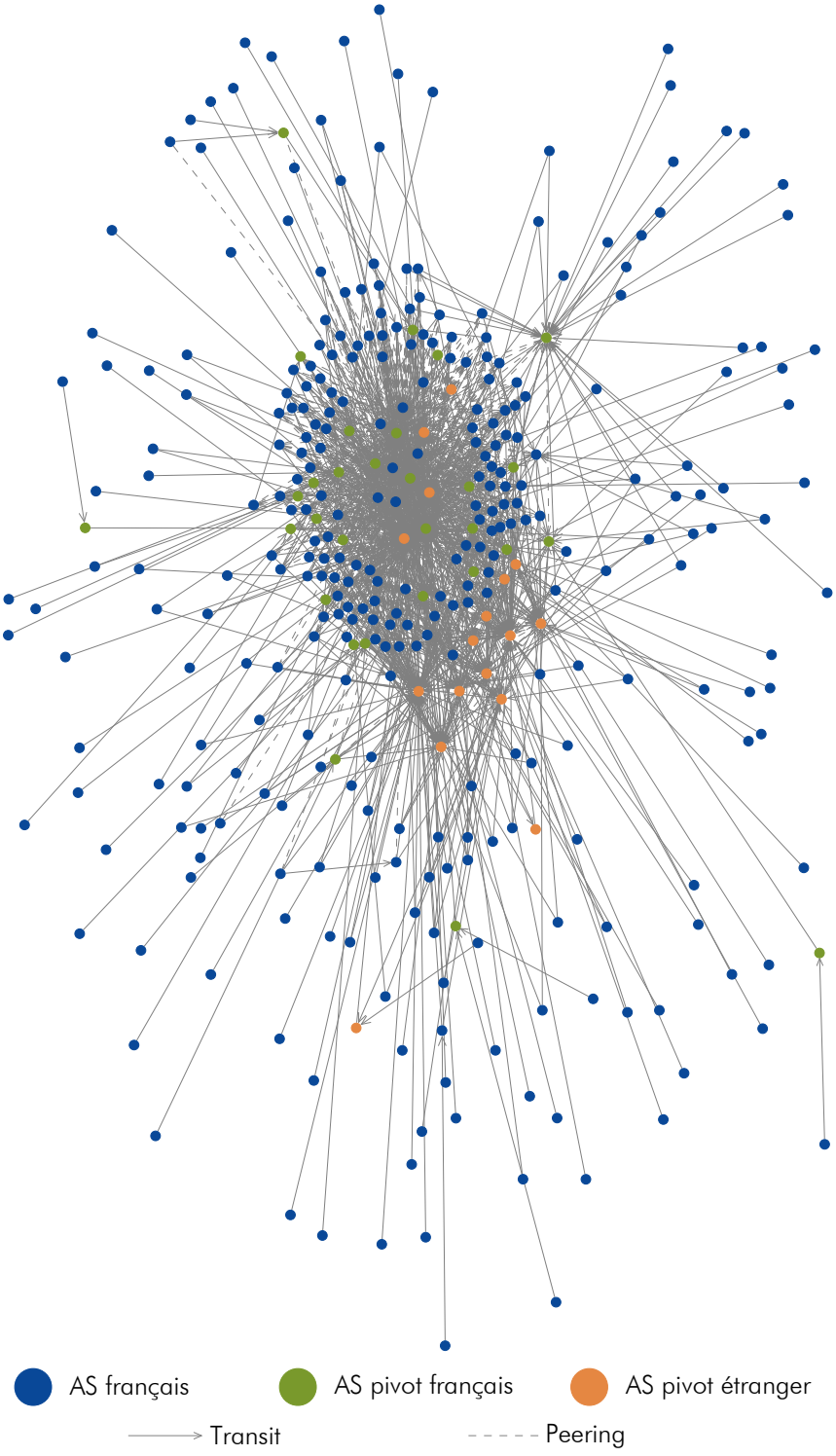

Figure 1.5 – Graphe de connectivité en IPv6 (décembre 2016)

Impacts de la disparition d'un AS

Les nombres d'AS pivots français et étrangers, donnés par la figure 1.6, ont très légèrement augmenté en IPv4 et IPv6.

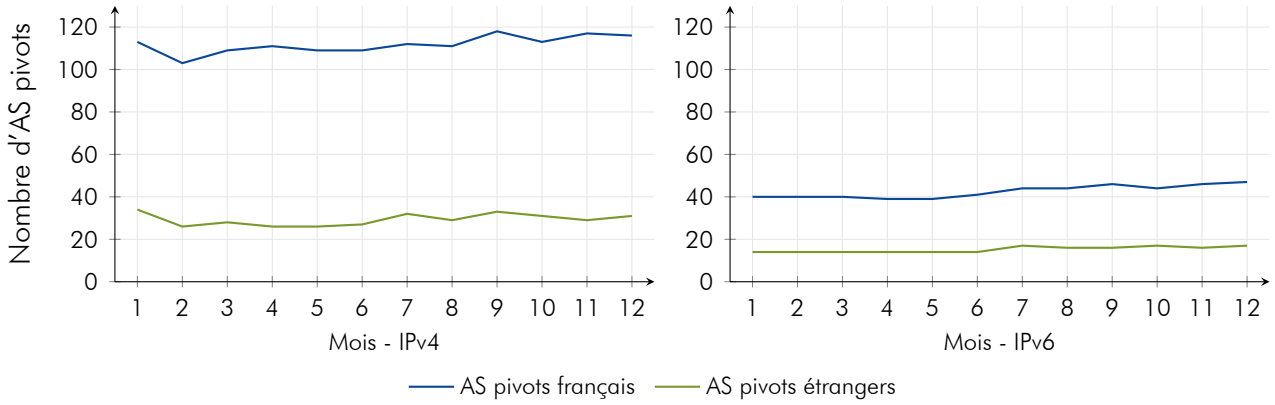

Figure 1.6 – Évolution du nombre d'AS pivots français et étrangers en 2016

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 8 AS pivots affecteraient au moins 10 AS en cas de défaillance. Le nombre d'AS pivot a augmenté par rapport à l'année 2015. L'AS pivot le plus critique aurait un impact sur 48 AS, contre 42 en 2015. 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 2015, le nombre d'AS pouvant être déconnectés a augmenté. Il s'agit d'un

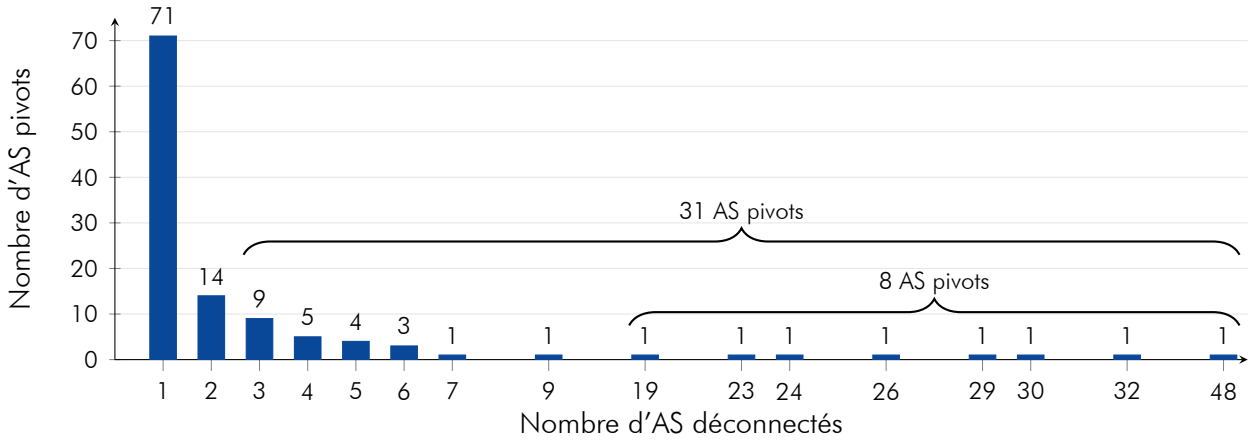

Figure 1.7 – AS pivots en fonction du nombre d'AS déconnectés (IPv4, déc 2016)

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

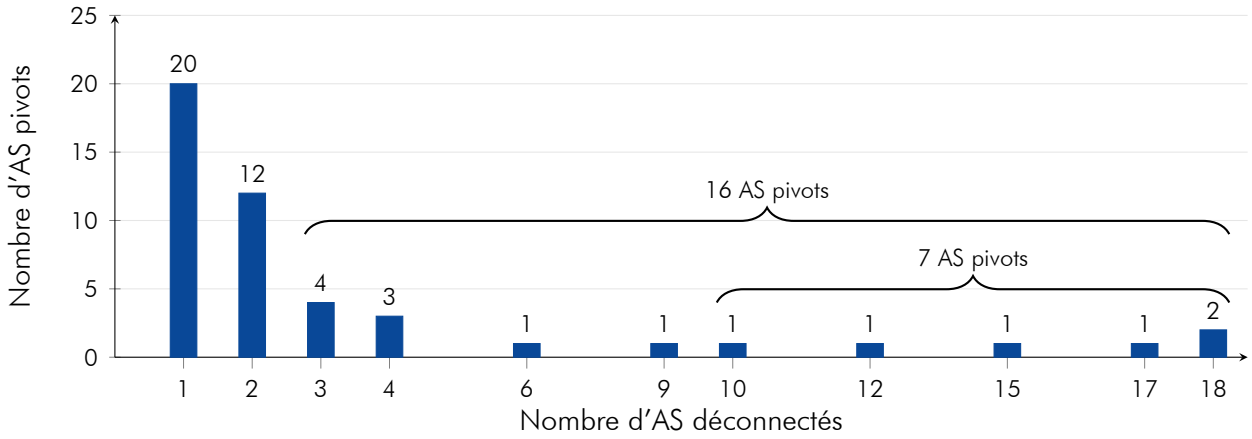

Figure 1.8 – AS pivots en fonction du nombre d'AS déconnectés (IPv6, déc 2016)

1.3 Usurpations de préfixes

Une usurpation est l'annonce via BGP d'un préfixe IP par un opérateur qui n'en est pas le délégataire légitime. Un conflit est l'annonce via BGP d'un préfixe IP déjà annoncé par un autre opérateur (ou couvert par un préfixe moins spécifique). Un conflit n'est pas systématiquement une usurpation. L'enjeu de la détection d'usurpation est de trouver tous les conflits puis de les tamiser pour en extraire les événements anormaux.

L'observatoire a mis en oeuvre des filtres automatiques et manuels pour qualifier les conflits détectés quotidiennement à partir d'archives BGP publiques. La figure 1.9 montre la répartition des conflits après la première phase de filtrage. Les conflits *valides* sont légitimes, parce qu'un objet route est déclaré. Ceux en catégorie *relation* ont une information commune pour les deux AS impliqués, comme une appartenance à la même organisation. Enfin, les conflits *directs* concerne les AS connectés directement l'un à l'autre pour lesquels une usurpation de préfixe est peu probable.

Le nombre de conflits détectés au cours de l'année 2016 est similaire au nombre de conflits détectés en 2015, avec néanmoins une légère baisse. En tout, 5951 conflits ont touché 320 AS français.

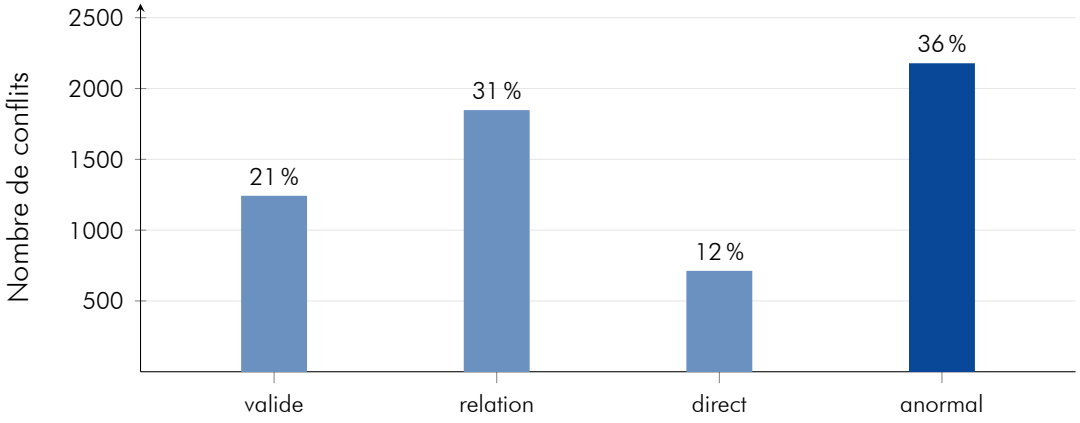

Figure 1.9 – Types de conflits détectés en 2016

Par rapport à 2015, même si les conflits "anormaux" représentent toujours environ le tiers des conflits, le nombre total de conflits a baissé d'environ 10 %. De plus, les conflits "valides" ont significativement diminué, passant de 49 % à 21 %. Il est difficile d'attribuer cette baisse à un changement particulier, mais deux tendances peuvent l'expliquer :

- l'amélioration de la couverture des objets `route` et des `ROA` associée à la mise en œuvre du filtrage par les opérateurs qui pourrait avoir limité la progression des conflits BGP.
- les préfixes non couverts par des objets `route` ou `ROA` ont été plus souvent la cible de conflits. Cette hypothèse est la plus probable puisqu'il y a eu un report des conflits "valides" vers la catégorie "relation", qui passe de 10 % à 31 %.

Au final, 2171 conflits anormaux doivent faire l'objet d'une analyse plus poussée pour tenter d'identifier des usurpations de préfixes.

1.3.1 Réannonces de table globale

Les réannonces de table globale apparaissent à la suite d'erreurs de configuration des routeurs BGP. Un AS peut alors annoncer des préfixes qui ne lui appartiennent pas. Elles se caractérisent par un nombre de conflits important à l'origine d'un même AS sur une courte période.

L'observatoire a développé un algorithme dans le but de les détecter automatiquement. Il vise à modéliser celles-ci 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 ;
- une augmentation significative 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, sans pour autant sélectionner de faux positifs.

En effet, l'algorithme détecte 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, il ne reste plus que 47 AS à l'origine de réannonces de table globale. La visualisation des séries temporelles représentant le nombre de préfixes annoncés par jour, et le nombre d'AS en conflit par jour pour ces 47 cas, permet de valider ce résultat.

Certains de ces 47 AS ayant fait des réannonces plusieurs fois en 2016, ces résultats correspondent à 50 réannonces de table globale dans l'année soit plus de 4 par mois. Parmi ces 47 AS, seulement 7 ont été en conflit avec des AS français aux dates où les réannonces de table globale ont été détectées, impactant 19 AS français au total.

L'AS étant entré en conflit avec le plus d'AS français (soit avec 15 d'entre eux) à la suite d'une réannonce de table globale est un AS suisse. Il a annoncé plus de 3200 préfixes supplémentaires, entrant en conflit avec au total près de 700 AS, le 22 avril 2016. Le cas a été rendu public et selon bgpmon.net [15], il est également à l'origine d'un cas attribué à un AS privé. Cet AS privé est lui rentré en conflit avec 17 AS français, le même jour.

Les autres cas détectés ont impacté beaucoup moins d'AS français (3 au maximum) et n'ont pas été rendus publics. Cependant, un grand nombre d'entre eux est entré en conflit avec plusieurs dizaines et jusqu'à plus d'une centaine d'AS dans le monde.

Sur les 2171 conflits anormaux, 286 conflits correspondent à des réannonces de table globale. Ces résultats permettent ainsi de traiter automatiquement une partie conséquente des conflits détectés.

1.3.2 Filtrage automatique des conflits anormaux

Les filtres introduits lors de l'édition 2015 du rapport pour faciliter l'analyse ont permis d'écarter 1827 des conflits anormaux. Ainsi, les conflits qui sont parvenus à moins de 10 pairs BGP ont une faible visibilité et sont écartés. C'est le cas d'environ 200 conflits.

De même, un filtrage des annonces trop spécifiques pour être considérées comme ayant une visibilité sur Internet a aussi enlevé 875 conflits. Ces conflits ont, entre autres, concerné un opérateur russe qui a annoncé des adresses IP de serveurs appartenant à des sites de jeux d'argent en ligne, à une plateforme de blog populaire et quelques dizaines de clients d'un hébergeur de serveurs dédiés.

Les conflits utilisant des numéros d'AS réservés ou visant des préfixes spéciaux n'ont pas été considérés. Ce sont donc 180 conflits de plus qui ont été retirés automatiquement.

Lorsque les deux opérateurs à l'origine d'un conflit sont tous les deux français, nous considérons qu'ils peuvent communiquer directement pour résoudre l'incident. En cas de problème persistant, ils sont en mesure d'assigner juridiquement l'autre opérateur. Nous ignorons donc de tels conflits et écartons environ 180 autres conflits.

1.3.3 Analyse manuelle des conflits restants

Une analyse manuelle est nécessaire pour classer les 56 conflits anormaux restants. On constate de nombreux transferts de ressources, AS ou préfixes, vers une entité différente. Ainsi, une quinzaine de conflits ont été causés par ces migrations, qui durent généralement de quelques minutes à quelques jours, pendant lesquels le nouveau et l'ancien délégataire de la ressource les annoncent en même temps.

Enfin, près de la moitié des conflits anormaux restants sont de probables erreurs de manipulation ou de configuration. Comme rapporté dans l'édition 2015, le préfixe d'interconnexion d'un point d'échange français a été à nouveau annoncé par un de ses membres. L'opérateur a annoncé le préfixe pendant une courte durée. Des transitaires, qui fournissent aussi des protections contre le DDoS, ont annoncés sporadiquement des préfixes de certains de leurs clients alors que ceux-ci continuaient de les annoncer.

1.3.4 Usurpations de préfixes

Finalement, 18 conflits sont notablement anormaux et méritent une analyse manuelle poussée. Il ressort de cette analyse que les fournisseurs d'hébergement, offrant notamment la location de serveurs dédiés, sont les principales victimes des usurpations. Ainsi, un FAI régional américain a usurpé, pendant plusieurs jours, et avec des annonces plus spécifiques (/24), les préfixes de trois fournisseurs d'hébergement européens. Un de ces fournisseurs a été touché au moins 7 fois par des usurpations différentes. L'une des usurpations est particulièrement évidente puisque le chemin d'AS est complètement

faussé pour apparaître comme venant d'Afrique du sud alors que les transitaires ont des numéros d'AS en Grande Bretagne et en Chine.

Plusieurs préfixes d'une filiale africaine d'un opérateur mobile français ont été usurpés, pendant plusieurs jours, par un opérateur notoirement connu pour être à l'origine d'annonces BGP illégitimes, dont les activités avaient déjà été exposées dans la version précédente du rapport.

1.4 Utilisation des objets route

Les bonnes pratiques veulent 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 étude 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 couverts par un objet `route`.

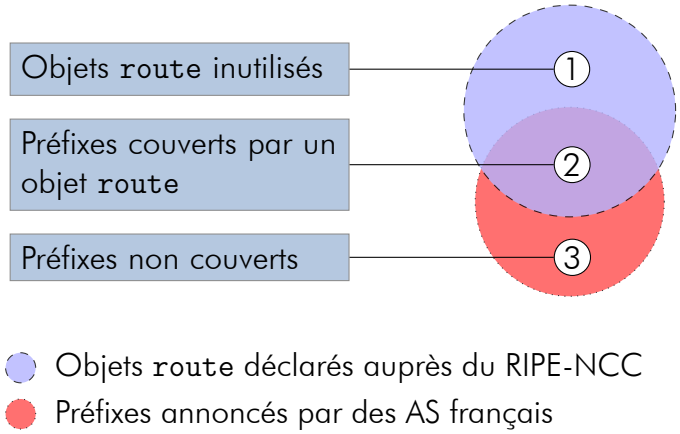

Figure 1.10 – Représentation des sous-indicateurs de l'utilisation des objets `route`

Objets route inutilisés

L'étude ici porte sur les objets `route` pour lesquels aucun préfixe n'a été annoncé au cours de l'année. Ils étaient 1626 en début d'année pour terminer à 2035 au 31 décembre. Cette croissance inhabituelle s'explique par une déclaration importante d'objets `route`, près de 250, le 31 mars par un réseau universitaire gérant plusieurs AS. Pour IPv6, les objets `route6` sont passés de 228 à 251.

À retenir

En 2016, beaucoup d'objets `route` ont été créés. L'usage supposé d'une grande partie consiste en un changement d'attribution d'`inetnum` entre plusieurs AS dans les mois à venir.

	Type	1er janvier	31 décembre
IPv4	aucun objet `route` déclaré	653	592
	aucun objet `route` utilisé	95	111
IPv6	aucun objet `route6` déclaré	1259	1199
	aucun objet `route6` utilisé	134	150

Table 1.1 – Répartition des AS selon l'usage des objets `route` en 2016

Les AS sont étudiés selon deux catégories représentées dans le tableau 1.1 :

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

L'évolution de cette répartition est très proche de celle de l'année passée. Pour IPv4, les AS sans objet `route` diminuent de 61 tandis que le nombre d'AS n'utilisant aucun objet `route` passe de 95 à 111. Pour IPv6, la tendance est la même, une diminution de 60 AS dans la catégorie des AS sans objet `route6` déclaré, tandis que 16 AS se sont ajoutés à l'ensemble des AS n'utilisant aucun des objets `route6` déclarés.

Préfixes non couverts par des objets route

Contrairement à 2015, la situation se dégrade. De 815 préfixes IPv4 non couverts début 2016, l'année se termine avec 849 préfixes dans cette catégorie. Pour IPv6, le nombre de préfixes non couverts est passé de 117 à 144. Le nombre de préfixes annoncés a grandement augmenté en 2016. Sur la totalité des nouveaux préfixes annoncés sur l'année, 14 % de ces derniers n'ont pas d'objets `route` déclarés.

Les AS ayant tous leurs préfixes couverts sont passés de 802 à 829 pour IPv4. Pour les AS dont au moins un objet `route` fait défaut, 48 AS se sont ajoutés, terminant à 184 au 31 décembre. Pour IPv6, 242 AS avaient tous leurs objets `route6` déclarés en début d'année pour finir à 282. La quantité d'AS annonçant des préfixes IPv6 ayant au moins un objet `route6` manquant a évolué de 47 à 56.

À retenir

Même si la situation s'améliore pour la couverture des préfixes IPv4 et IPv6 annoncés par des objets `route`, l'application des bonnes pratiques pour les déclarations n'est pas systématique pour certains AS et reste un axe d'amélioration important.

1.5 Déclarations dans la RPKI

Évolution de la couverture de l'espace d'adressage

Au début du mois de janvier 2016, 231 AS français avaient des ROA dans la RPKI. À la fin de l'année 2016, ce nombre est passé à 255, montrant une augmentation du nombre d'AS participants. Cette augmentation de 10 % est plus faible que celles observées les années précédentes : en 2015, le nombre d'AS participants avait connu une croissance de 20 % au cours de l'année.

L'évolution de la couverture de l'espace d'adressage IPv4 géré par les AS français au cours de l'année 2016 a été étudiée. Les pourcentages de l'espace d'adressage valide, invalide et non couvert ont peu évolué au cours de l'année. Au 31 décembre 2016, le pourcentage de l'espace d'adressage valide était de 66 %, c'est-à-dire légèrement supérieur à celui observé en 2015 (65 %). Par ailleurs, le pourcentage de l'espace d'adressage invalide est inférieur à 1 % à la fin de l'année. Enfin, le pourcentage d'adressage non couvert est d'environ 33 % au 31 décembre 2016. Ces dernières valeurs sont comparables à celles observées en 2015.

Les observations concernant le protocole IPv6 montrent qu'il n'y a pas eu d'évolution au cours de l'année 2016. Ainsi, au 31 décembre 2016, à l'instar des années précédentes, moins de 1 % de l'espace d'adressage est couvert par les ROA.

Validité des annonces effectuées par les AS français

Afin d'estimer l'impact potentiel d'un filtrage strict sur la connectivité, l'étude a également porté sur le nombre d'AS effectuant uniquement des annonces de préfixes valides ou invalides.

Au cours de l'année 2016, le nombre d'AS effectuant uniquement des annonces de préfixes valides a très faiblement augmenté, passant de 128 AS au début de l'année à 133 AS au 31 décembre. En comparant ces valeurs à la croissance du nombre d'AS participant à la RPKI, on constate que la proportion d'AS effectuant uniquement des annonces de préfixe valides a baissé au cours de l'année 2016.

L'analyse des annonces de préfixes montre qu'un seul AS a été vu effectuant uniquement des annonces de préfixes invalides, 3 fois au cours de l'année. En réalité, cet AS n'a pas été actif le reste de l'année. Il est possible que les annonces de préfixes invalides, de courtes durées, aient été causées par la mise en service d'un équipement dont la configuration n'avait pas été mise à jour.

Par ailleurs, l'étude montre que les déclarations de ROA de certains LIR [15] rendent des annonces de préfixes de leurs clients invalides. Par exemple, un LIR annonce le préfixe

15. Local Internet Registry.

198.18.0.0/15 et a déclaré un ROA autorisant son annonce, mais interdisant celle de préfixes plus spécifiques. Si ce LIR a assigné le préfixe 198.18.0.0/17 à un de ses clients, ce dernier effectuera une annonce invalide selon la RPKI, car provenant d'un AS autre que celui du LIR, et plus spécifique que la longueur maximale autorisée. Au 31 décembre 2016, un peu moins de 20 AS sont affectés par ce type de déclarations.

Utilisation potentielle de la RPKI par les AS français

Les mesures 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 de préfixes permet d'obtenir un aperçu de la maintenance effectuée sur les ROA dans le temps.

	Type	1er janvier	31 décembre
Nombre d'AS (IPv4)	Aucun ROA utilisé	18	30
	Quelques ROA utilisés	35	42
	Tous les ROA sont utilisés	172	181
Nombre d'AS (IPv6)	Aucun ROA utilisé	11	14
	Quelques ROA utilisés	5	8
	Tous les ROA sont utilisés	65	78

Table 1.2 – Évolution de l'utilisation des ROA

Le tableau 1.2 donne des indications relatives à la cohérence des ROA par rapport aux annonces de préfixes au début et à la fin de l'année 2016. À l'instar du constat effectué sur l'année 2015, une part importante des AS utilisent tous leurs ROA. Au cours de l'année, on constate une augmentation du nombre d'AS n'effectuant aucune annonce de préfixe conforme aux ROA déclarés dans la RPKI.

À retenir

En fin d'année 2016, un bilan semblable à celui des années précédentes peut être établi : un tiers de l'espace d'adressage IPv4 n'est pas couvert par la RPKI. En ce qui concerne IPv6, la couverture reste inférieure à 1 % de l'espace d'adressage.

Chapitre 2

Résilience sous l'angle du protocole DNS

2.1 Introduction

Les noms de domaine gérés par le protocole DNS [1] [16, 17], sont organisés dans une base de données hiérarchique et répartie. L'objectif principal de ce système de nommage 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 `192.134.5.24`. 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 juste en dessous de la racine, comme `.fr`, sont appelés des noms de premier niveau (TLD [2]).

À chaque niveau se trouvent 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.

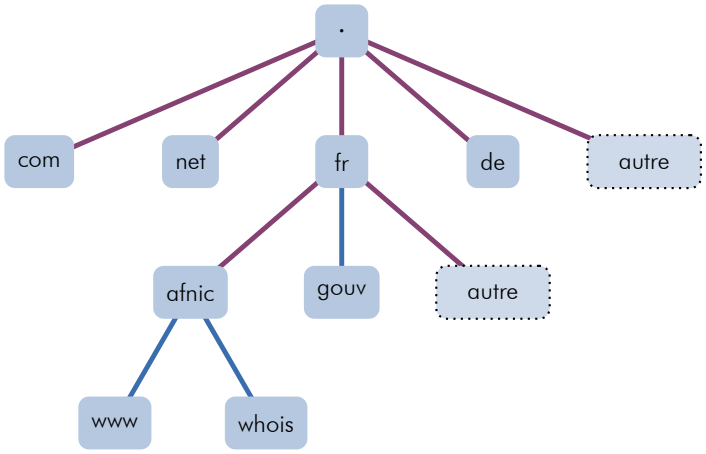

Figure 2.1 – Structure du DNS

1. Domain Name System.
2. Top Level Domain.

Une zone peut être « déléguée » afin de confier la gestion de ses données à un organisme 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 [3]. 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 [4] dans un registre dédié aux paramètres du DNS [18]. 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 ;
- `DS` et `DNSKEY` : des informations cryptographiques utiles pour DNSSEC [5].

Interroger le DNS

La résolution DNS est le mécanisme qui permet de récupérer les enregistrements associés à un nom et à un type donnés. Elle 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 [6], interroge l'arborescence DNS en partant de la racine (interaction 2) et en suivant 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. Ils peuvent faire autorité pour le nom de domaine demandé par le serveur récursif, auquel cas ils lui retournent la réponse. Dans le cas contraire, ils l'aiguillent vers d'autres serveurs à interroger qui seraient plus susceptibles de faire autorité pour le nom de domaine recherché.

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

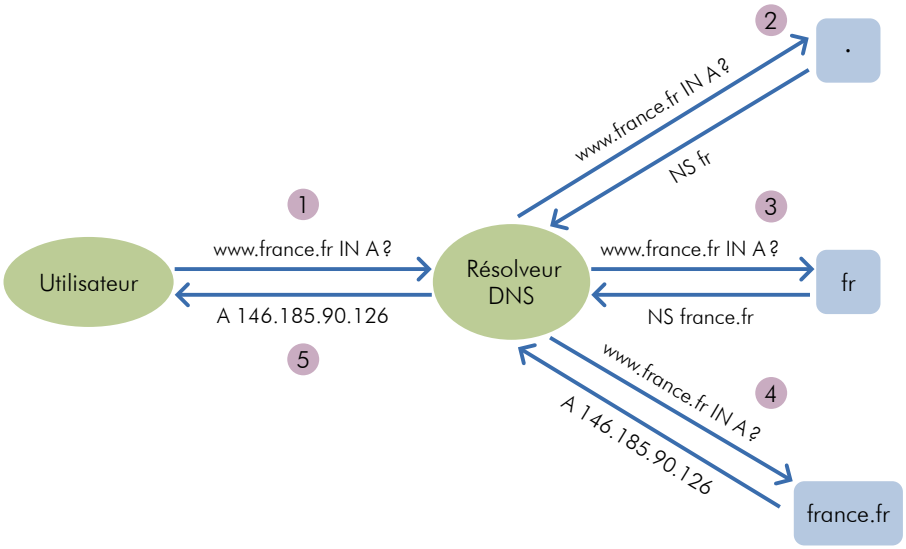

Figure 2.2 – Exemple de résolution DNS

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, ici `ssi.gouv.fr`, est l'emplacement dans l'arbre DNS de cet enregistrement. Le nom à droite, comme ici `dns1.ssi.gouv.fr`, est la donnée. Ce nom doit généralement être résolu 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.

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 [7], pouvant impliquer 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 [8] pendant trois semaines [19], 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 la PSL [9] [20]. Cette liste provient d'une initiative de Mozilla pour renforcer le cloisonnement logique des sites web dans les navigateurs. Bien que n'ayant pas un rapport direct avec le DNS, elle 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 lors de sa création. Le protocole DNSSEC [21] 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 `DS`. Ce mécanisme empêche notamment les attaques dites de « pollution de cache » visant à injecter des enregistrements frauduleux dans un serveur cache.

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

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` [22] 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. Plus un serveur héberge de zones, plus sa probabilité d'être choisi pour résoudre un domaine est faible.

Si le serveur interrogé 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 dont les réponses sont invalides ou n'ayant pas répondu à nos requêtes ne sont pas comptés dans les statistiques. Ils constituent un biais de près de 4 % des noms de domaine délégués de la zone `.fr` en décembre 2016, soit environ 117 617 noms de domaine. En décembre 2015, ce biais était de 3 %, soit 77 500 noms de domaine. Cette augmentation peut être due à l'emploi, cette année, d'un serveur récursif validant DNSSEC.

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 celles pour lesquelles l'ensemble des mesures ont pu être conduites sans échecs, sont comptabilisées. Elles sont appelées les « zones étudiées ». Ainsi, de 2015 à 2016, le nombre de ces zones a augmenté de 1 % pour atteindre environ 2 840 000 à la mi-décembre 2016, contre environ 2 810 000 au 7 décembre 2015. Cette évolution est due à la création de 556 000 nouvelles zones, à la suppression de 525 000 zones et à l'augmentation du nombre de zones en échec lors des mesures.

Il importe de noter que les données utilisées font autorité. Cela signifie que les enregistrements 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 et la base de données Geolite de Maxmind ont été téléchargées en décembre 2016.

Les dates de création des zones étudiées sont obtenues par l'analyse des données publiques de l'Afnic, publiées dans le cadre de l'initiative OpenData [23].

2.2 Dispersion des serveurs DNS faisant autorité

Nombre de serveurs par zone déléguée

Le nombre d'enregistrements NS par zone étudiée a faiblement évolué entre décembre 2015 et décembre 2016, comme le montre la figure 2.4. Seule une légère diminution du nombre de zones n'ayant que deux enregistrements NS est observée, ainsi qu'une augmentation proportionnelle du nombre de zones ayant trois à quatre enregistrements. Cette variation s'explique par la dynamique du marché, avec la part croissante d'un fournisseur de services employant plus d'enregistrements NS pour désigner ses serveurs DNS.

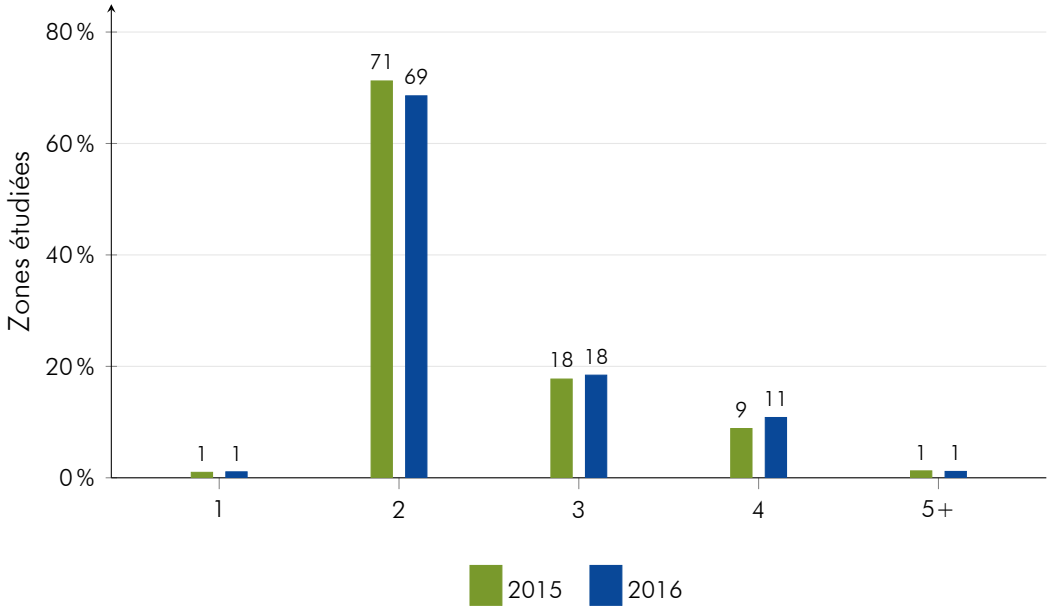

Figure 2.4 – Nombre d'enregistrements NS par zones étudiées

Le nombre d'enregistrements NS par zone déléguée reste suffisant pour permettre une bonne résilience, du point de vue de cet indicateur. En effet, environ 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, la répartition est sensiblement équivalente à celle observée lors de l'étude des enregistrements NS. En IPv6, 63 % des zones étudiées disposent d'au moins un enregistrement NS dont le nom peut être résolu en adresse IP. Cette situation est légèrement meilleure qu'en 2015, où la proportion de ces zones n'était que de 59 %. Parmi ces zones disposant d'adresses IPv6, environ 25 000 domaines disposent d'un ou plusieurs enregistrements NS dont les noms de serveurs DNS sont résolus en plusieurs adresses IP. Ainsi, en IPv6, la dispersion topologique des serveurs DNS se révèle être meilleure que ce qui aurait pu être observé par la seule étude

des enregistrements NS. En particulier, 14 % de ces zones peuvent être résolus auprès de quatre adresses IPv6.

Si ces résultats concernant IPv6 sont encourageants, il convient de noter que près de 37 % des zones ne disposent d'aucun serveur ayant une adresse IPv6. Elles reposent donc exclusivement sur la disponibilité de serveurs en IPv4.

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 progressé en 2016. Ainsi, environ 37 % des zones ne sont accessibles qu'en IPv4, contre 41 % en 2015.

Dispersion topologique des zones déléguées

La dispersion topologique des serveurs DNS est une exigence issue de l'ingénierie de la résilience [24, 25]. La dispersion des serveurs de noms dans des AS distincts peut, dans certains cas, contribuer à éviter des indisponibilités en cas d'incident sur le réseau d'un opérateur. En 2016, le nombre moyen d'AS par zone reste équivalent à celui de 2015, et stagne à 1,2. Par ailleurs, la quantité de zones hébergées par un seul AS reste stable depuis 2011, culminant à 83 % des zones étudiées.

La dispersion des serveurs DNS 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.

À retenir

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

Dispersion géographique des serveurs DNS faisant autorité

La dispersion géographique des serveurs DNS faisant autorité peut avoir un impact sur la disponibilité des services de l'Internet français. Par exemple, cela peut être le cas à la suite d'une 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 [26], 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'adresse 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.

En 2016, le nombre de zones étudiées étant servies exclusivement par des serveurs faisant autorité situés dans un même pays a diminué, par rapport à 2015. Ce phénomène est observé tant en IPv4 qu'en IPv6. Ainsi, en IPv4, ce taux est passé de 82 % à 80 %. En IPv6, le taux est passé de 82 % à un peu moins de 81 %. Pour les deux protocoles, cette évolution est expliquée par une diminution du nombre de zones étudiées étant exclusivement hébergées en France. Il ne s'agit cependant pas systématiquement d'un phénomène d'émigration des zones étudiées, mais aussi parfois d'une augmentation de la diversité géographique.

En 2016 et en IPv4, les zones dont tous les serveurs DNS faisant autorité sont dans un même pays étranger représentent 28 % des zones étudiées, contre 27 % en 2015. Il convient néanmoins de noter que 68 % d'entre elles sont hébergées dans un pays ayant une frontière terrestre avec la France métropolitaine. Ce dernier taux a diminué de quatre points de pourcentage entre 2015 et 2016 [10]. Cette situation ne présente, a priori, pas un risque significatif, mais la tendance observée en 2016 est à surveiller ; elle indique, en effet, une migration des zones étudiées vers des plateformes d'hébergement situées à l'étranger, et en particulier en Amérique du Nord. Le taux de zones dans cette situation a ainsi augmenté, d'un peu moins de 20 % des zones étudiées en 2015, à un peu plus de 21 % des zones étudiées en 2016.

En 2016 et en IPv6, la même tendance peut être observée. Ainsi, les zones hébergées dans un seul pays étranger représentent 31 % des zones ayant des serveurs DNS accessibles en IPv6 en 2016 contre 30 % en 2015. Cette faible augmentation ne rend cependant pas apparent le fort changement dans la liste des pays où sont hébergées ces zones. En effet, alors qu'en 2015, 85 % de ces dernières étaient hébergées dans un pays frontalier de la France métropolitaine, celles-ci ne représentent en 2016 que 79 %. À l'inverse, le nombre de zones hébergées en Amérique du Nord a augmenté sur la même période, passant de 6 % à 15 %.

10. Le rapport 2015 contenait une erreur, ayant évalué ce taux à 75 % au lieu de 72 %.

À retenir

La dispersion géographique des zones étudiées est globalement satisfaisante, tant en IPv4 qu'en IPv6. Néanmoins, près de 21 % des zones sont servies en IPv4, exclusivement depuis l'Amérique du Nord. En IPv6, le pourcentage de zones servies exclusivement depuis l'Amérique du Nord a augmenté significativement entre 2015 et 2016. La migration des zones étudiées vers des pays étrangers et en particulier en Amérique du Nord nécessite d'être suivie.

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. Cette statistique n'a pas évolué entre 2015 et 2016.

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 87 % 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`, par exemple `.net`. Cette statistique a diminué de deux points de pourcentage entre 2015 et 2016 ; cette variation ne semble pas suffisamment marquée pour être significative.

De même, en 2015 comme en 2016, 75 % des zones étudiées ont deux degrés de dépendance, dus 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

L'évolution du nombre de zones disposant d'au moins un enregistrement DS a été observée en utilisant les zones étudiées du 6 décembre 2015 et du 19 décembre 2016. Pour simplifier, le terme *zone DNSSEC* est utilisé pour désigner ces zones.

Entre 2015 et 2016, le pourcentage de zones DNSSEC a dépassé la barre symbolique des 10 %, ayant crû de 8,8 % à 10,2 %. En décembre 2016, il est ainsi possible de dénombrer environ 291 000 zones.

Afin de déterminer l'origine de cette évolution, il est intéressant de détailler la croissance de la zone `.fr`. Ainsi, 556 000 zones ont été créées entre décembre 2015 et décembre 2016. Cela représente 20 % des zones étudiées fin 2016. Pendant la même période, environ 525 000 zones ont été supprimées, soit 19 % des zones étudiées en décembre 2015.

Comparativement, les zones DNSSEC sont composées d'environ 99 000 zones nouvellement enregistrées, soit 34 % des zones DNSSEC en décembre 2016. En outre, environ 71 000 zones ont été supprimées de la zone `.fr`, soit 28 % des zones DNSSEC en décembre 2015.

Au-delà de la dynamique de croissance des zones DNSSEC, il est intéressant de souligner qu'environ 21 000 zones déjà enregistrées en 2015 ont mis en œuvre DNSSEC en 2016. Par ailleurs, environ 6400 zones signées en 2015 ont désactivé DNSSEC au cours de l'année. Ces zones représentent 3 % des zones DNSSEC en 2015.

La croissance de DNSSEC est donc essentiellement due aux créations de zones. Ainsi, à peine 1 % des zones étudiées, qui existaient déjà en 2015, ont mis en œuvre DNSSEC au cours de l'année 2016.

À retenir

Un peu plus de 10 % des zones étudiées mettent en œuvre DNSSEC en 2016. Comme en 2015, la croissance est essentiellement due à la création de nouvelles zones en 2016.

Analyse des algorithmes cryptographiques

Comme en 2015, près de 92 % des zones étudiées et disposant d'un enregistrement DS indiquent 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 obsolète SHA-1, tel qu'employé dans la suite cryptographique `RSASHA1-NSEC3-SHA1`, est contraire aux bonnes pratiques actuelles communément admises en cryptographie [27], et aux recommandations du RGS [11] [28]. En particulier, une attaque pratique en collision contre SHA-1 a pu être démontrée en 2017 [29].

L'analyse des algorithmes employés pour hacher les clés DNSSEC des zones étudiées contraste avec le résultat précédent. Ainsi, en 2015 comme en 2016, 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 SHA-1, un algorithme de hachage obsolète. 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 étudiée

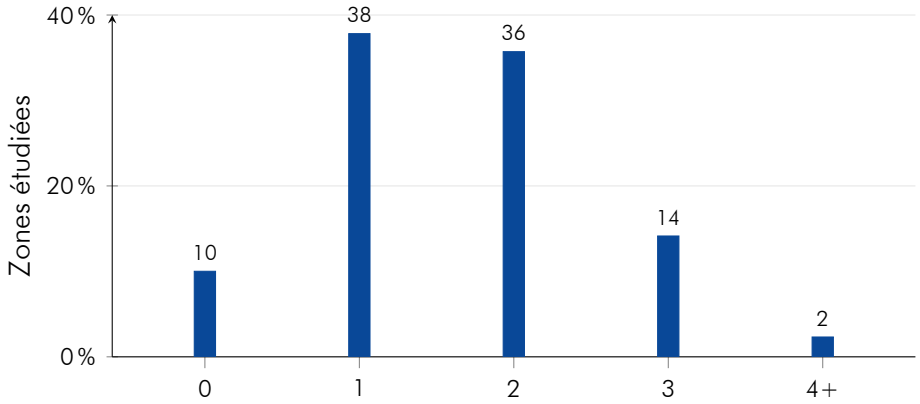

Figure 2.5 – Nombre de relais de messagerie entrants par zone en 2016

En 2016 et comme les années précédentes, 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 2.5. Cette statistique est constante, depuis 2014. 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.

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.

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 quasiment identique au nombre d'enregistrements MX, comme l'illustre la figure 2.6. Le cas particulier détecté en 2015, concernant une plateforme d'hébergement qui associait cinq adresses IPv4 à un nom de domaine utilisé

dans un enregistrement MX secondaire [12], a cependant modifié le nombre d'adresses IP associées à ce nom. Il n'est désormais retourné qu'une seule adresse IP, réduisant ainsi à quasiment zéro le nombre de zones disposant de plus de six relais de messagerie. En 2016, une autre plateforme a cependant pris la relève, retournant trois adresses IP pour un même nom. Ainsi, pour environ 10 % des zones, quatre adresses IPv4 peuvent être contactées pour leur délivrer des courriers électroniques. Les zones employant cette plateforme de service bénéficient donc d'une plus grande résilience, puisqu'elles disposent d'au moins quatre adresses IPv4 au total.

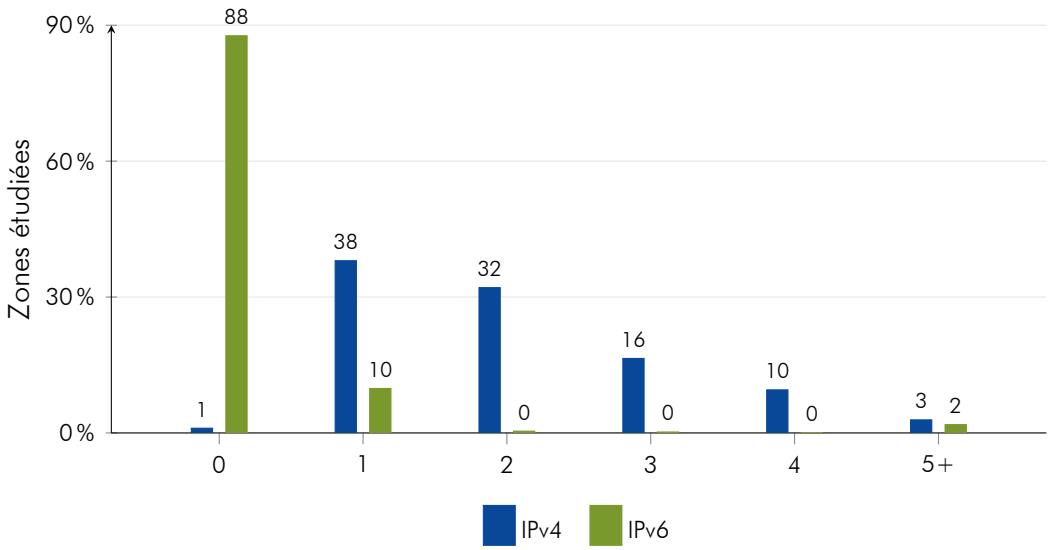

Figure 2.6 – Nombre d'adresses IP de relais de messagerie entrants par zone en 2016

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 88 % des zones, aucun des enregistrements MX n'a d'adresse IPv6 associée. La situation s'est donc marginalement améliorée ente 2015 et 2016, avec une réduction de ce nombre de l'ordre d'un point de pourcentage. Parmi les 12 % restants, pour 80 % de ces zones, un seul nom contenu dans les enregistrements MX

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.

peut être résolu en une unique IPv6. Ici aussi, il s'agit d'une amélioration marginale de la situation, de l'ordre d'un point de pourcentage, par rapport à 2015.

Il est intéressant de noter qu'une plateforme de service a un comportement atypique. Cette dernière représentait 10 % des zones dont les relais disposent d'adresses IPv6 en 2015 et culmine désormais à 14 %. 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`. Le nombre d'adresses IPv6 potentiellement associées aux noms de domaine dont les relais de messageries sont hébergés sur cette plateforme peut monter jusqu'à 28.

À retenir

IPv6 reste peu déployé. Ainsi, pour 88 % des zones, aucun des enregistrements MX n'a d'adresse IPv6 associée. Parmi les 12 % restants, pour 80 % 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.

En 2016 et comme les années précédentes, 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 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 70 % d'entre elles, ce TLD est `.net` et pour 20 %, 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 [30].

Un degré de dépendance est également introduit pour les 22 % de zones utilisant des noms de serveur – relais de messagerie – dans un unique domaine hors juridiction, toutefois 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.

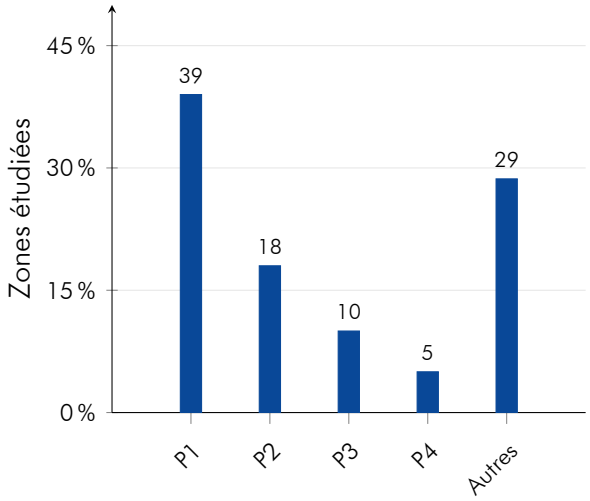

Figure 2.7 – Concentration des relais de messagerie sur des plateformes, en 2016

À retenir

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

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 2 160 000 zones [13].

Comme le montre la figure 2.7, 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, comme en 2015.

13. Le nombre de zones renseigné dans le rapport 2015 pour cette statistique était erroné, à cause d'une erreur dans la fonction de calcul. En 2015, le nombre de zones était également de 2 160 000.

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 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.

En IPv4, concernant les zones étudiées et disposant d'enregistrements MX, 98 % d'entre elles utilisent des relais de messagerie tous situés dans un même pays. Cela représente donc environ 2 430 000 zones et une amélioration marginale par rapport à 2015 où le nombre de zones dans cette situation était de 2 540 000. En IPv4, comme en 2015, 69 % de ces zones ont leurs relais localisés en France. Le seul pays hors de l'Europe et contenant un nombre significatif de relais de messagerie est les États-Unis d'Amérique, avec 5 % des zones concernées.

En IPv6, il convient de rappeler que près de 88 % des zones ne disposent d'aucun relais de messagerie en IPv6. Seules 316 000 zones sont donc concernées par cette étude. Ainsi, 86 % de ces zones utilisent des relais de messagerie tous situés dans un même pays. Pour 243 000 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.

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 95 % 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 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 43.

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. L'approche utilisée en 2015 était d'additionner par numéro d'AS les adresses IP des relais de messagerie de chaque domaine. Ainsi, si une adresse IP est indiquée comme relais de messagerie dans deux domaines, elle était comptabilisée deux fois pour ce numéro d'AS.

Ainsi, en 2016 et en IPv4, 28 % des relais de messagerie sont concentrés au sein d'un unique AS, contre 47 % en 2015. Cette diminution est expliquée par le fait que les chiffres étaient artificiellement gonflés en 2015, par l'emploi de cinq adresses IPv4 pour l'un des relais de messagerie secondaire opéré par cet hébergeur. À l'inverse, en 2016, deux opérateurs ont gonflé leurs chiffres en suivant le même procédé. Le premier répond désormais trois adresses pour l'un des relais de messagerie secondaire qu'il héberge, et accroît ainsi sa part de 9 % à 14 %. Le second est l'opérateur qui répond une seule adresse IP mais qui est distincte en fonction du serveur qui est interrogé. Ce faisant, ce dernier représente 18 % des relais de messagerie cette année, contre 9 % en 2015. Ces pratiques remettent donc en doute le bien-fondé de cette statistique, introduite dans le rapport 2015.

La nouvelle méthode de calcul tient compte du nombre de domaines hébergés partiellement ou totalement par un AS. Ainsi, si un domaine dispose de trois relais de messageries, deux dans un AS, et le dernier dans un autre AS, le compteur du premier AS sera augmenté de 0,66, et le compteur du second AS de 0,33. Cette façon de comptabiliser permet ainsi de s'abstraire du nombre d'adresses IP par enregistrement MX ; seule l'importance relative d'un AS dans l'hébergement des relais de messagerie d'une zone étudiée est alors considérée.

Avec cette nouvelle méthode, il apparaît une stabilité entre 2015 et 2016. L'AS hébergeant le plus de relais de messagerie rend disponible sur Internet environ 38 % d'entre eux, contre 37 % en 2015 ; le second ne représente que 16 % en 2016.

Par ailleurs, quatre opérateurs hébergeurs regroupent à eux seuls 66 % des relais de messagerie des zones étudiées.

Avec la nouvelle méthode de calcul et en IPv6, la concentration observée est bien plus forte qu'en IPv4, puisque 69 % des relais sont hébergés par un même acteur. Le deuxième acteur en héberge quant à lui 15 %.

À retenir

La concentration des relais de messagerie entrants sur quelques opérateurs réseau est significative. En IPv4, un opérateur est responsable de la connectivité de 38 % 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 [1] 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 [31, 32, 33] depuis la conception du protocole SSL [2], désormais obsolète [34]. 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 [3] retenue pour la session étant déterminée grâce aux messages de type `handshake`.

Sans se substituer aux références plus précises [35, 36], 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 RSA ou ECDSA au sein d'un certificat numérique ;
4. le serveur transmet dans un `ServerKeyExchange` une valeur aléatoire 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 aléatoire qu'il transmet dans un `ClientKeyExchange` ;

1. Transport Layer Security.
2. Secure Sockets Layer.
3. En anglais, *cipher suite*.

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.

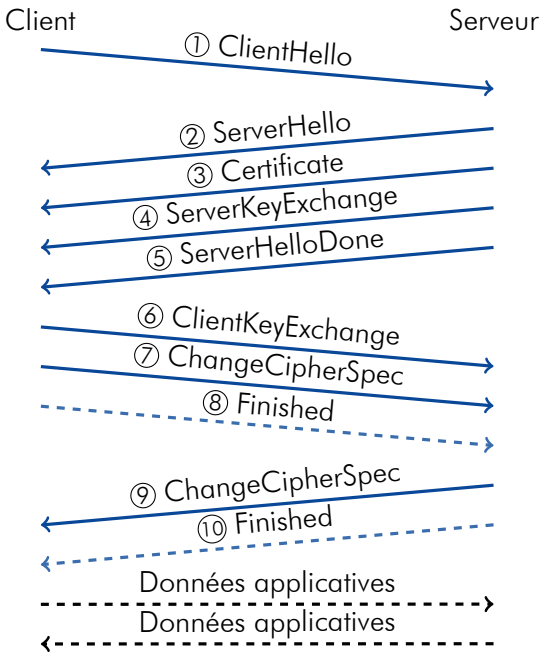

Figure 3.1 – Initiation générique d'une session TLS

Le cas générique décrit ici sous-entend l'adoption d'une des suites cryptographiques qui assurent la propriété de confidentialité persistante, ou PFS [4]. Celle-ci consiste à prévenir le déchiffrement de messages de sessions passées quand bien même la clé privée (RSA ou ECDSA) du serveur serait compromise. Elle passe par la négociation d'un secret éphémère à l'aide d'un échange Diffie–Hellman [37].

Les spécifications du protocole définissent par ailleurs plusieurs messages supplémentaires et extensions qui permettent d'encadrer et d'enrichir la protection des communications [38]. 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 formulent cette validité et la maintiennent représente une IGC.

4. Perfect Forward Secrecy.

Pour un certificat conforme à la norme X.509 [39] suivie dans le cadre de TLS, l'assurance que la clé publique qu'il contient appartient 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 [5] 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 [40]. 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 encourage à suivre le guide de recommandations de sécurité relatives à TLS [41], qui synthétise l'annexe A4 du RGS [42].

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 [43] et ne sont pas abordés dans le présent rapport.

Les noms de domaine issus du registre maintenu par l'Afnic [6] 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 entrecroisées à l'aide de Concerto [44]. Cet outil est par ailleurs en mesure de vérifier, et éventuellement de reconstruire, les chaînes de certificats observées. L'examen plus précis de certains certificats tire parti de la prise en charge du standard X.509 par Scapy [45].

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

L'extension SNI[7] [38] 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 effet, dans les contextes d'hébergement mutualisé, lorsque plusieurs domaines sont hébergés à la même adresse IP, il devient nécessaire de préciser un nom de domaine via l'extension SNI afin d'accéder aux ressources associées.

L'étude de l'ensemble des ressources est rendue complexe par l'existence de certains serveurs hébergeant plusieurs dizaines de milliers de domaines. Les efforts nécessaires pour réaliser des mesures pareillement exhaustives ne sont pas forcément valables. Des mesures parcellaires montrent qu'un tel travail permettrait de recenser un plus grand nombre de certificats X.509, mais que les paramètres de négociation TLS demeurent globalement constants parmi les domaines hébergés à une même adresse.

Pour cette raison, notre étude comptabilise de façon unique les adresses IP issues des résolutions du registre de l'Afnic. La figure 3.2 représente l'évolution du nombre de ports 443 ouverts parmi les adresses IP uniques visitées. Sur un nombre d'adresses stabilisé autour de 250 000 en 2016, la proportion de ports 443 ouverts a augmenté tout au long de l'année, pour atteindre près de 65 % au mois de décembre.

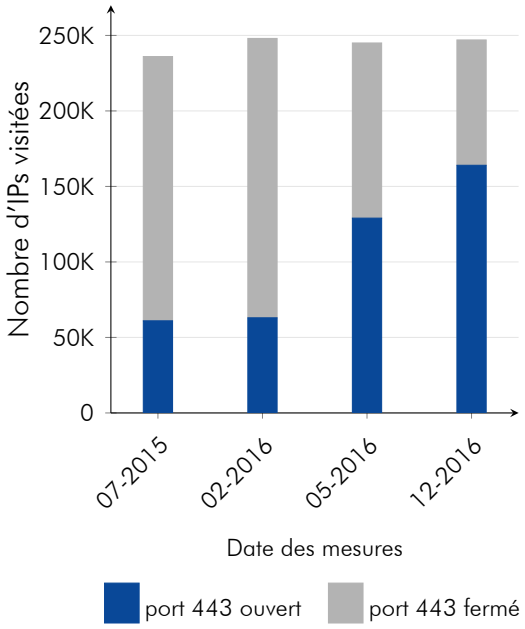

Figure 3.2 – Évolution du nombre d'adresses IP uniques visitées pour les mesures

7. 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 2016, tandis que d'autres ont été déclarés obsolètes car sujets à des attaques [46, 34]. Les attributs établis via la phase de négociation ont donc un impact direct sur la sécurité des échanges subséquents. Pour cette raison, l'observatoire cherche 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 année après année permettent cependant un constat qualitatif du respect des bonnes pratiques.

État général des serveurs TLS

En 2016, considérant l'ensemble des stimuli tentant de négocier une session TLS 1.0 ou TLS 1.2 (avec des variations notamment au niveau des suites cryptographiques proposées), 73 % des serveurs présentant un port 443 ouvert permettaient d'initier une session TLS. Par ailleurs, seuls 2,2 % des serveurs n'envoyaient aucune donnée quel que soit le stimulus utilisé, et 0,3 % répondaient des données jamais reconnues en tant que messages TLS.

Le pourcentage de serveurs acceptant au moins une négociation, en baisse par rapport aux 80 % observés mi-2015, s'attribue en partie au nombre croissant de serveurs qui exigent une extension SNI pour l'établissement d'une connexion TLS, et qui n'étaient pas mesurables avec notre méthodologie. Cette diminution relative ne doit pas occulter la croissance absolue du nombre de serveurs prenant bien en charge TLS.

Prises en charge comparées de TLS 1.0 et TLS 1.2

La figure 3.3 précise les taux de succès d'établissement de session lors de la campagne de mesure principale avec TLS 1.2 en 2015 et 2016, dont le stimulus proposait plusieurs suites cryptographiques sans contrainte particulière. 71 % des serveurs sont aptes à négocier une session TLS 1.2, en légère diminution par rapport aux 75 % de 2014.

Cette évolution est liée à l'absence d'extension SNI, qui se manifeste d'ailleurs par l'augmentation du nombre d'alertes TLS reçues. La proportion de messages non reconnus est passée de 8 % à 5 % ; un examen manuel révèle une majorité de pages HTML non chiffrées.

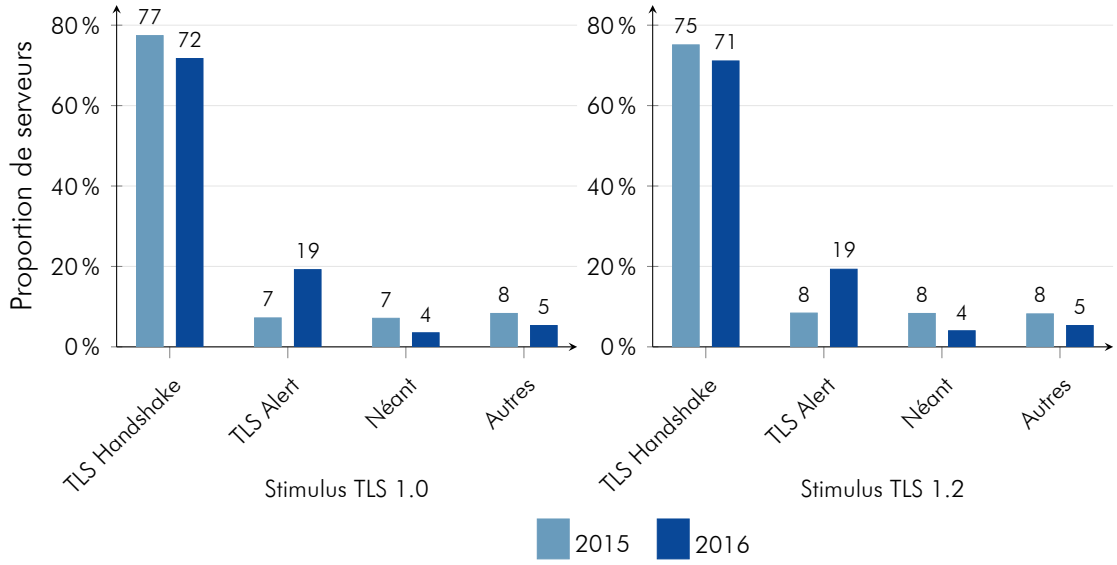

Figure 3.3 – Évolution des réponses des serveurs HTTPS aux stimuli TLS 1.0 et 1.2

Ces observations diffèrent de moins de 1 % des résultats obtenus à l'issue de la campagne principale menée pour TLS 1.0. Bien qu'une majorité des clients web prenne désormais en charge TLS 1.2, l'interopérabilité avec des clients datés est presque immanquablement maintenue. La version 1.2 protège toutefois les communications de certaines attaques de complexité moyenne qui peuvent affecter la version 1.0 [47].

À retenir

TLS 1.2 est couramment pris en charge par les serveurs de la zone `.fr` en 2016. 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 [8] et ECDHE [9] 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. À la mi-2015, parmi les serveurs capables de négocier une quelconque session TLS 1.0 ou TLS 1.2, près de 92 % offraient déjà la confidentialité per-

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

sistante. Cette proportion a augmenté à 95 % en 2016, confirmant une large adoption des échanges de clé DHE ou ECDHE.

Cette tendance positive doit toutefois être tempérée par le fait que la tolérance à DHE ou ECDHE ne garantisse pas qu'un tel 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. Pourtant, en 2016, seuls des navigateurs particulièrement anciens ne prennent pas en charge ces méthodes. En fonction des parts de clients web utilisés par les visiteurs d'un site, il peut être approprié de renforcer la sécurité des connexions à l'aide d'une telle règle.

À retenir

En 2016, l'offre de confidentialité persistante via HTTPS est largement répandue 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 [46]. SSLv2 est désactivé par défaut dans les navigateurs web récents, tandis que sa dangerosité continue d'être évaluée à la hausse [48].

La figure 3.4 représente les réponses des serveurs de la zone `.fr` ayant reçu un `ClientHello` SSLv2. Le message est ignoré par 78 % des serveurs mi-2015, et par 93 % des serveurs fin 2016.

Bien qu'il existe un code d'erreur permettant de rejeter les versions de protocole non prises en charge, seul 1 % des serveurs répondait avec un message de type `alert` en 2016. Dans la mesure où les structures binaires des messages SSLv2 et TLS sont largement différentes, il est compréhensible que la prise en charge exclusive de TLS par un serveur empêche de reconnaître les messages formatés selon SSLv2, et aboutisse à une absence de réponse.

Ainsi, moins d'un serveur sur vingt accepte de monter une session SSLv2. Rapportée aux nombres respectifs de serveurs mesurés en 2015 puis en 2016, l'évolution se traduit en absolu par une diminution de la prise en charge de SSLv2 de près de 3000 serveurs. La version obsolète, en plus de ne pas être prise en charge par les nouveaux serveurs, disparaît progressivement des installations existantes.

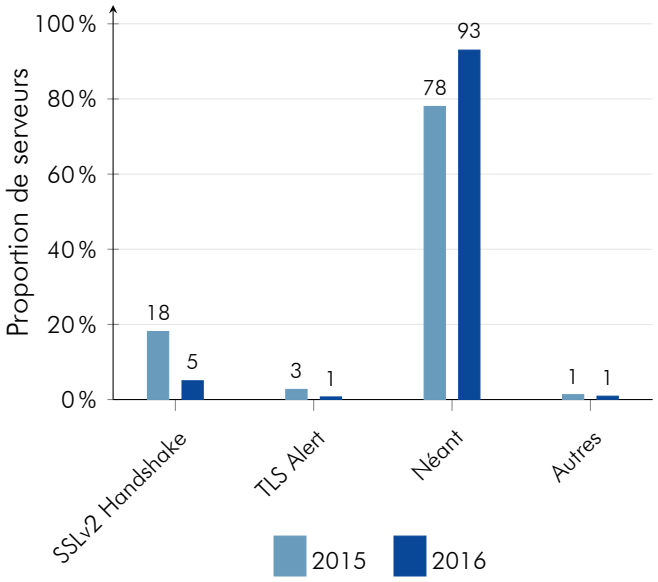

Figure 3.4 – Réponses des serveurs français à un stimulus SSLv2

À retenir

En 2016, la prise en charge de la version SSLv2 a significativement diminué sur les serveurs web. Sa disparition doit être menée à terme.

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.

Historiquement, la fonction de hachage la plus répandue était SHA-1. Cependant, plusieurs attaques théoriques contre cette fonction ont été mises au jour depuis 2005 [49, 50], poussant notamment les éditeurs de navigateurs web à planifier l'obsolescence de cette fonction dans le cadre des IGC. Début 2017, la dangerosité de SHA-1 a été entérinée par la démonstration d'une attaque de collisions pratique [29].

L'abandon de la fonction de hachage par les navigateurs a été graduel. Dès 2015, la visite des sites qui s'appuyaient sur SHA-1 était généralement accompagnée d'un avertissement peu intrusif à l'attention de l'internaute [51]. Au cours du premier semestre 2017, les principaux éditeurs de navigateurs déploieront une page interstitielle pour décourager la consultation de tels sites [52, 53, 54].

Évolution des signatures 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'a 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. Près de 90 000 certificats distincts ont tout de même été relevés lors des mesures menées fin 2016, ce qui permet d'identifier des tendances significatives.

La proportion de certificats auto-signés est en baisse : de 41 % en 2015, elle est passée à 31 % l'année suivante. 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 2016 en faisant abstraction des certificats auto-signés, qu'ils soient reconnus ou non par des magasins de confiance publics.

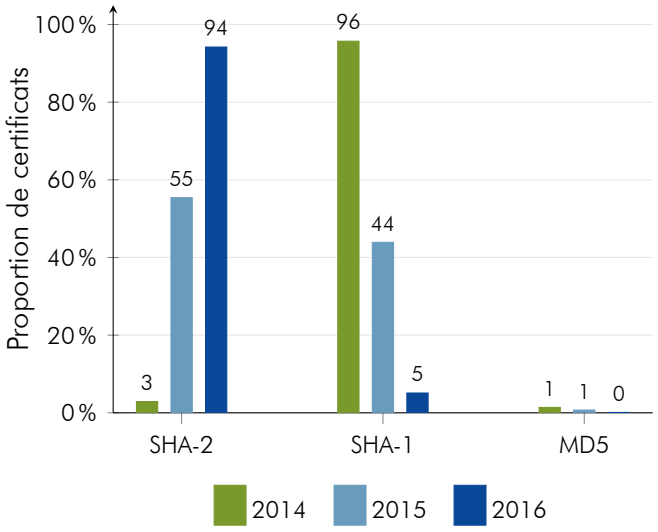

Figure 3.5 – Évolution des signatures des certificats

Début 2014, la part de certificats non expirés signée à l'aide de SHA-2 était de 3 % seulement, tandis que 96 % d'entre eux étaient signés avec SHA-1. Fin 2016, les proportions sont inversées, avec 94 % de SHA-2 contre 5 % de SHA-1.

En excluant les certificats les plus anciens de l'analyse, l'adoption de SHA-2 est encore plus affirmée. En effet, plus de 98 % des certificats valides au plus tôt le 1er janvier 2016 (qui peuvent être assimilés aux certificats émis au cours de l'année 2016) sont signés avec SHA-2. Ainsi, grâce à l'appui des éditeurs de navigateurs, la transition est en passe d'être intégrale.

Le résidu de certificats signés avec MD5 s'est quant à lui presque évanoui : ils ne représentent plus que 0,1 % des certificats observés en 2016. L'algorithme MD5 est vulnérable à des attaques de collisions pratiques depuis au moins 2004 [55], et son usage à des fins cryptographiques est à proscrire. Un examen manuel des adresses IP concernées confirme qu'il s'agit essentiellement de serveurs non utilisés, renvoyant des pages HTML vides ou laissées par défaut.

À retenir

Les certificats HTTPS signés avec SHA-1, bientôt rejetés par les principaux navigateurs, ont presque disparu. Conformément aux bonnes pratiques, le nouveau standard s'appuyant sur SHA-2 est largement adopté.

Chapitre 4

Étude des sources de DDoS en France

Introduction

Des services mis en œuvre sur des équipements connectés à Internet peuvent être exploités pour mener des attaques DDoS. L'observatoire a mené une étude sur les sources de DDoS par amplification au sein de l'Internet français. Ces attaques exploitent les propriétés de certains protocoles afin de générer un volume de trafic important ou un grand nombre de de paquets par seconde dans le but de saturer les capacités de traitement d'une cible [4]. Afin de limiter le risque de participation à une attaque DDoS par amplification, il est important de prendre certaines précautions et de mettre en œuvre, le cas échéant, des contre-mesures.

La surface d'attaque peut être réduite en désactivant les services obsolètes ou inutilisés, ou en veillant à ce que ceux-ci soient inaccessibles sur le réseau en les faisant écouter sur une interface locale ou au moyen de règles de pare-feu.

Certains services peuvent être exposés sur Internet alors qu'ils ne devraient pas l'être. C'est notamment le cas de SSDP (*Simple Service Discovery Protocol*) [56], qui n'a pas vocation à être utilisé en dehors d'un réseau local, ou encore celui de la résolution DNS récursive. Il est important de s'assurer que de tels services ne peuvent pas répondre à des requêtes provenant de l'Internet. D'une manière générale, l'interrogation de services doit être restreinte aux réseaux autorisés à le faire.

Lorsque des services ont vocation à être exposés sur Internet, des règles de limitation de débit peuvent réduire le risque de participation à une attaque par déni de service. Par exemple, un mécanisme de type RRL (*Response Rate Limiting*) [57] peut être mis en œuvre sur les serveurs DNS faisant autorité.

Par ailleurs, les bonnes pratiques de configuration des services et protocoles mis en œuvre doivent être appliquées. Par exemple, le protocole SNMP permet d'administrer et de superviser des équipements au moyen de l'envoi de requêtes spécifiant une chaîne de caractère appelée communauté. Dans les versions antérieures à la version 3, la sécurité de ce protocole reposait sur la connaissance des communautés. Ces dernières doivent donc être traitées comme des mots de passe. En particulier, les chaînes par défaut (*public* pour la lecture, *private* pour l'écriture) doivent être modifiées. Par ailleurs, l'accès aux équipements *via* le protocole SNMP doit également être restreint au réseau d'administration ou de supervision. En outre, l'usage de la version 3 du protocole

SNMP (niveau de sécurité `authPriv`) doit être privilégié.

Bien que les attaques par amplification aient été nombreuses au cours des dernières années, il ne s'agit pas du seul vecteur utilisé pour mener des DDoS. Les applications web peuvent comporter des vulnérabilités susceptibles d'être exploitées pour mener des attaques DDoS [58]. Afin de limiter la surface d'attaque et l'impact des tentatives de déni de service, les applications web ainsi que les *frameworks*, les CMS (*Content Management System*) et les greffons utilisés doivent être maintenus à jour. Par ailleurs, le développement de ces applications doit suivre les bonnes pratiques. Un audit de code peut révéler des failles qui pourraient être exploitées par des attaquants. Pour plus d'informations, le lecteur peut consulter les recommandations de l'ANSSI [59] concernant la sécurité des applications web.

Enfin, il est nécessaire de veiller à ce que les interfaces d'administration d'équipements connectés à Internet ne soient pas accessibles en dehors des réseaux d'administration. Dans le cas où celles-ci doivent être exposées sur Internet, il est nécessaire de prendre des précautions afin de limiter le risque de compromission :

- restreindre les adresses IP à partir desquelles il est possible d'y accéder ;
- désactiver les comptes par défaut, ou, au minimum, modifier les mots de passe par défaut.

Pour plus d'informations sur les attaques DDoS et les contre-mesures existantes, le lecteur peut consulter le guide « Comprendre et anticiper les attaques DDoS » de l'ANSSI [4].

Méthodologie de mesures

En 2016, l'ANSSI a effectué des mesures sur l'Internet français afin de recenser les équipements susceptibles de participer à une attaque en déni de service distribué [1] par amplification [4].

Depuis le mois d'avril 2016, des mesures sont effectuées régulièrement sur les protocoles suivants :

- DNS (UDP / 53) : requête pour un enregistrement `PTR` avec le bit `rd` ;
- NTP (UDP / 123) : requêtes mode 6 (messages de contrôle) et mode 7 (requêtes spécifiques à `ntpd` [60]) ;
- SNMP (UDP / 161) : requêtes `GetNextRequest` (SNMPv1) [61] et `GetBulkRequest` (SNMPv2c) [62] ;
- SSDP (UDP / 1900) [63] : requêtes de type `M-SEARCH`.

Les requêtes envoyées dans le cadre de ces mesures sont documentées sur la page web suivante : `http://www.anti-ddos-measurements.ssi.gouv.fr/`

1. En anglais : *Distributed Denial of Service*, ou DDoS.

Sur demande, les préfixes IP d'une société ou d'une organisation peuvent être exclus du périmètre des mesures.

Résultats et analyse

Afin d'avoir un aperçu de l'évolution, dans la durée, du nombre d'équipements potentiellement exploitables, les données des projets maintenus par Jared Mauch, l'*Open Resolver Project* [64], l'*Open NTP Project* [65], l'*Open SNMP Project* [66], et l'*Open SSDP Project* [67] ont également été analysées. Les résultats de ces analyses, au même titre que celles effectuées par l'ANSSI sur l'Internet français, ont fait l'objet de signalements ayant contribué à la baisse du nombre d'équipements exploitables depuis mi-2013.

DNS : résolveurs ouverts

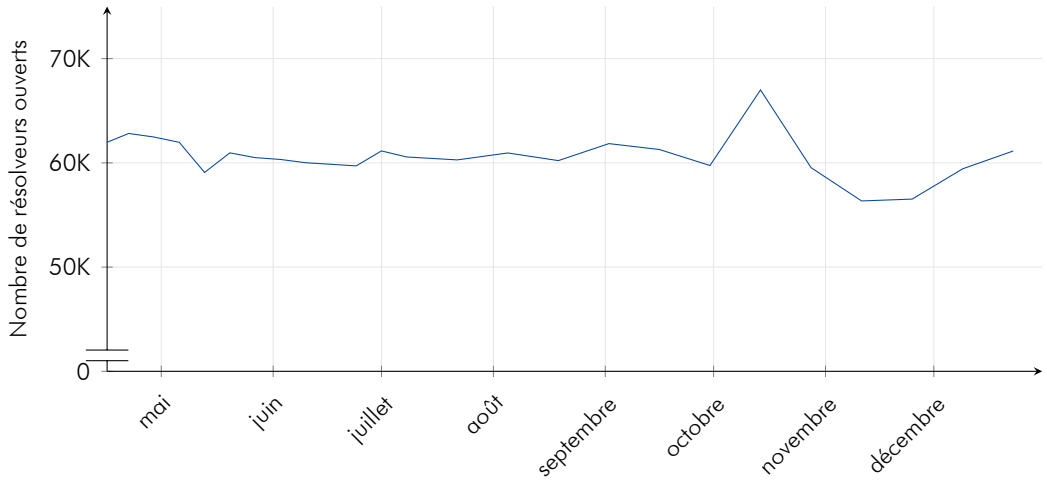

Figure 4.1 – Évolution du nombre de résolveurs DNS ouverts

À la fin de l'année 2016, l'Internet français comportait environ 60 000 résolveurs ouverts. Le graphe 4.1 montre que ce volume est resté globalement stable au cours de l'année 2016. Par ailleurs, l'analyse des données de l'*Open Resolver Project* permet de constater que cette valeur n'a pas évolué depuis la mi-2015.

En avril 2013, l'Internet français comptait, d'après l'*Open Resolver Project*, plus de 290 000 résolveurs ouverts, dont 70 % appartenaient à un seul AS. Ce nombre a connu une forte décroissance, d'environ 80 %, depuis les premiers recensements.

NTP : amplificateurs « mode 6 » et « mode 7 »

Certains messages NTP, appelés messages de contrôle ou requêtes de « mode 6 », permettent de lire des variables système. L'interrogation de serveurs NTP au moyen

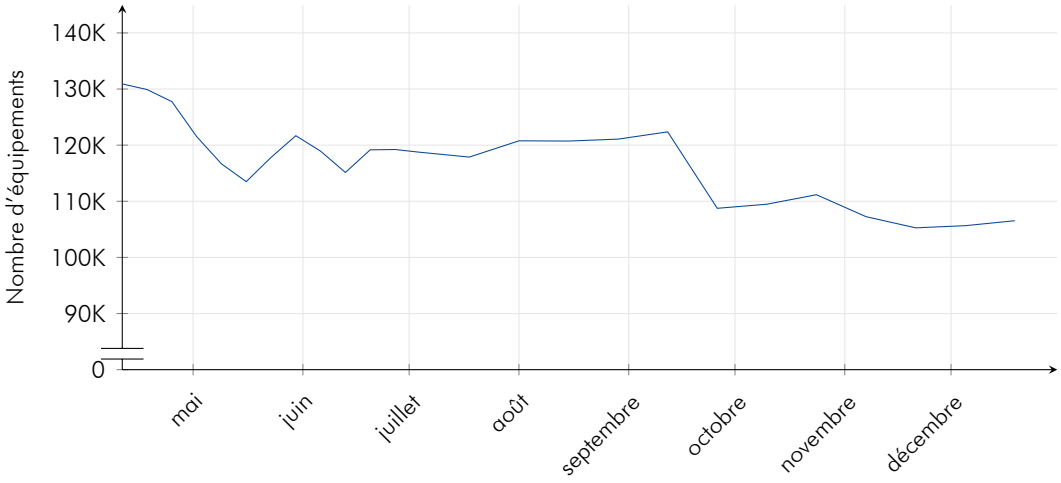

Figure 4.2 – Évolution du nombre d'amplificateurs NTP mode 6

de tels messages, par exemple avec la commande *readvar* [68], peut générer une amplification et donner des informations sur le système.

La figure 4.2 montre l'évolution du nombre d'amplificateurs NTP répondant à des requêtes de mode 6. À la fin de l'année 2016, l'Internet français en comporte plus de 100 000.

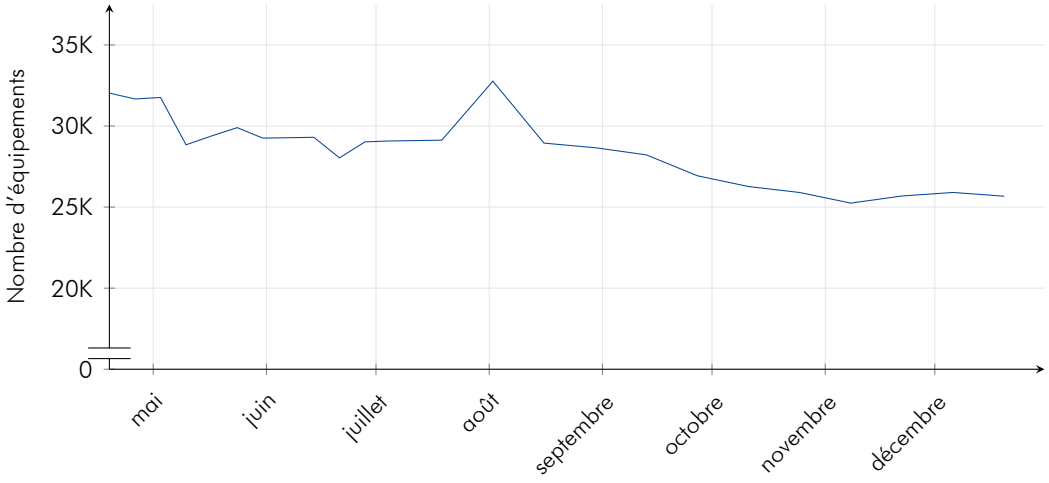

Figure 4.3 – Évolution du nombre d'amplificateurs NTP mode 7

Les amplificateurs dits « mode 7 » sont des équipements répondant à des requêtes de type *monlist* [69] proposées une implémentation du protocole NTP : *ntpd* [60]. La figure 4.3 montre que le nombre d'équipements répondant à ce type de requêtes a diminué au cours de l'année 2016. Au début de l'année, l'Internet français en comportait plus de 30 000. Ce nombre a baissé pour se situer aux alentours de 25 000 au cours du

mois de décembre 2016.

Le protocole SNMP

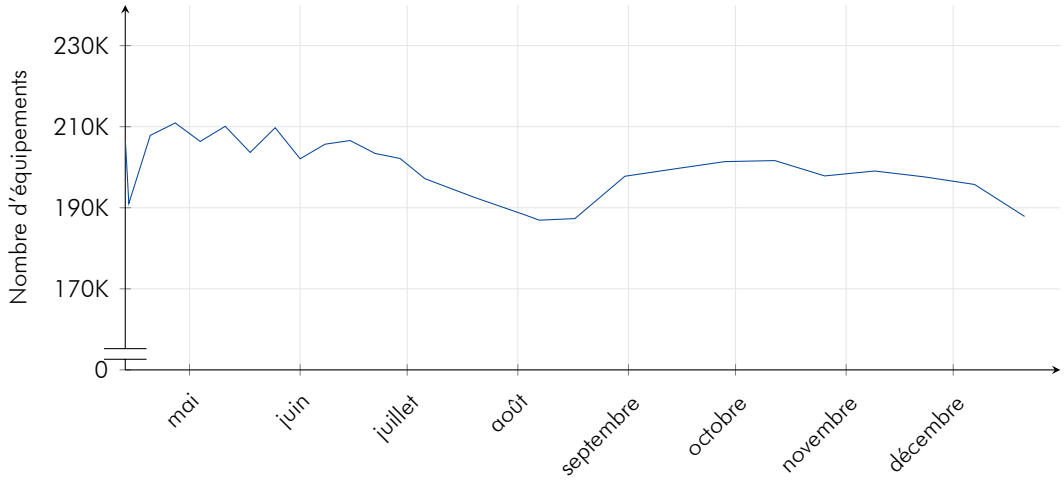

Figure 4.4 – Évolution du nombre d'équipements répondant à des *GetNextRequest*

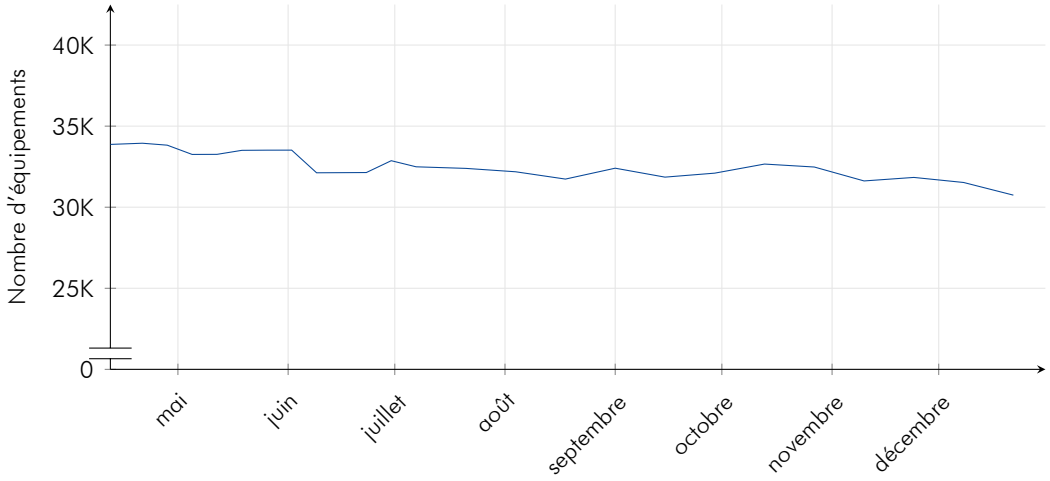

Figure 4.5 – Évolution du nombre d'équipements répondant à des *GetBulkRequest*

Le protocole SNMP est susceptible d'être exploité pour mener des attaques DDoS par amplification. En outre, une mauvaise mise en œuvre de ce protocole peut permettre d'obtenir des informations de configuration d'équipements.

À la fin de l'année 2016, l'Internet français compte plus de 200 000 équipements répondant à des requêtes SNMP pour la communauté en lecture par défaut (*public*). Parmi ceux-ci, un peu moins de 200 000 répondent à des `GetNextRequest` (graphe 4.4), et environ 30 000 répondent à des `GetBulkRequest` (graphe 4.5).

En décembre 2016, près de 75 % des équipements répondant à des `GetNextRequest` sont présents dans un seul AS. En ce qui concerne les `GetBulkRequest`, environ 33 % des équipements sont également concentrés dans un seul AS.

Amplificateurs SSDP

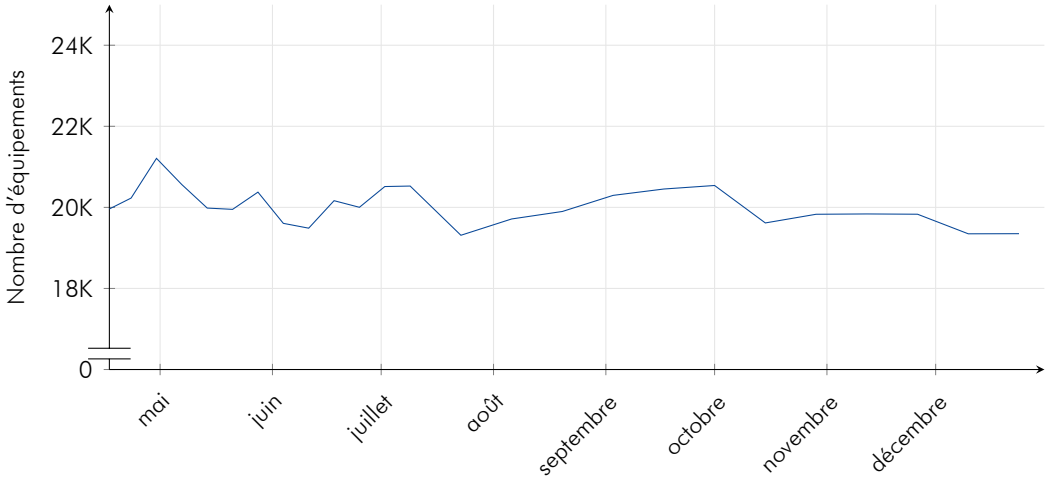

Figure 4.6 – Évolution du nombre d'équipements répondant à des requêtes SSDP

Le graphe 4.6 montre que le nombre d'équipements répondant à des requêtes SSDP n'a pas évolué significativement au cours de l'année 2016. À la fin de l'année, celui-ci se situe à près de 20 000 équipements. Par ailleurs, les analyses des données de l'*Open SSDP Project* [67] montrent que cette volumétrie est restée stable depuis 2015.

À retenir

À la fin de l'année 2016, l'Internet français comporte de nombreux équipements susceptibles d'être exploités pour mener des attaques en déni de service par amplification. Pour les protocoles observés, la volumétrie de ces équipements n'a pas évolué significativement au cours de l'année.

Conclusion générale

L'année 2016 a été particulièrement riche en ce qui concerne TLS. Dans un contexte de surveillances de masse mais aussi d'initiatives telles que Let's Encrypt, l'utilisation de HTTPS par les sites web français s'est accrue. En un an, la quantité de sites web accessibles en HTTPS est passée de 25 % à 65 %. La qualité des configurations des serveurs a aussi augmenté, permettant d'exclure des versions de protocole et des suites cryptographiques faibles, dont SSLv2 qui continue de disparaître. Au 1er janvier 2016 les certificats signés avec SHA-1 provoquaient une alerte de sécurité dans les navigateurs web. L'impact sur la signature des certificats a été particulièrement significatif car le nombre de certificats signés avec SHA-2 est passé de 55 à 94 %. La standardisation de TLS 1.3 touche à sa fin et devrait être terminée d'ici la fin de l'année 2017. L'équipe de l'observatoire espère que son adoption se fera aussi efficacement que celle observée pour SHA-2.

L'étude des vecteurs d'amplification et réflexion DDoS montre que la situation s'est stabilisée en France. Les signalements pour les protocoles tels que DNS, NTP, SSDP ou encore SNMP ont porté leurs fruits, amenant les responsables des équipements hébergeant ces services ouverts à déployer les correctifs nécessaires. Néanmoins, malgré ces opérations d'amélioration des parcs, de nouveaux équipements ajoutés dans les réseaux des opérateurs s'accompagnent parfois de ces services susceptibles d'être exploités pour des DDoS. C'est la raison pour laquelle le nombre d'adresses IP exploitables ne diminue pas de manière aussi importante qu'espéré. Des efforts doivent être faits par les entités qui corrigent des services ouverts pour reverser les correctifs dans les processus d'installation de nouveaux services.

Pour DNS, la zone .fr a tendance à stagner. Cependant, les indicateurs de ce protocole ont évolué comme par exemple la proportion des serveurs NS en IPv6. Ces derniers ont augmenté de 4 % sur l'année et sont majoritairement hébergés à l'étranger, l'augmentation du nombre de serveurs NS en IPv6 en France n'est pas significative. De plus, en ce qui concerne les serveurs NS, la tendance observée est qu'un grand nombre a déménagé vers l'étranger, notamment aux États-Unis. Les domaines en .fr signés par DNSSEC ont aujourd'hui dépassé 10 % de la zone .fr. Malgré cette augmentation de l'utilisation de DNSSEC, 92 % des zones utilisent l'algorithme SHA-1 qui est un algorithme obsolète et vulnérable à des attaques par collision. L'équipe de l'observatoire déplore ces résultats, déjà constatés lors de la rédaction du précédent rapport.

Les analyses des conflits d'annonces de préfixes en BGP ont permis de mettre en évidence 18 conflits anormaux. Parmi ces conflits, un opérateur américain a détourné pendant plusieurs jours des préfixes d'hébergeurs européens, mais aussi un opérateur

africain. Ce dernier s'était déjà fait remarquer pour des usurpations d'un opérateur mobile français dans le rapport précédent. L'analyse des objets `route` a montré des déclarations massives par un réseau universitaire semblant anticiper des mouvements d'adresses IP entre AS d'universités. Les déclarations d'objets `route` s'améliorent et des analyses poussées ont montré des destructions d'objets `route` suite à la cessation d'activité d'AS. Même si cela reste marginal, ces efforts sont notables. La RPKI dont l'objectif est de remplacer les objets `route` a en revanche peu évolué. Près d'un tiers des adresses IPv4 sont couvertes par des ROA tandis qu'en IPv6 moins de 1 % des adresses sont couvertes.

Depuis la création de l'observatoire, la promotion des bonnes pratiques sont au cœur des publications. Néanmoins, l'observatoire déplore que certaines bonnes pratiques font l'objet d'un suivi moins sérieux que d'autres. Ainsi, une amélioration particulièrement importante a été notée en ce qui concerne TLS, et une constance sur l'amélioration de la situation avec les déclaration des objets `route`. Mais, pour DNSSEC par exemple, la persistance de l'algorithme de hachage SHA-1 pour la signature des zones est inquiétante. De plus, IPv6 semble être considéré comme un réseau à part, c'est-à-dire ne semblant pas devoir faire l'objet de l'application systématiques des bonnes pratiques. L'équipe de l'observatoire tient à alerter les opérateurs qu'IPv6 doit faire l'objet d'autant d'attention, si ce n'est plus, qu'IPv4. Enfin l'observatoire renouvelle ses recommandations :

- **surveiller les annonces de préfixes** et se tenir prêt à réagir aux usurpations ;
- **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 ;
- **anticiper les attaques DDoS** en acquérant une solution de dépollution ou souscrire à une offre via un prestataire.

Bibliographie

[1] ANSSI, "Bonnes pratiques de configuration de BGP." <http://www.ssi.gouv.fr/bonnes-pratiques-bgp>, 2013.

[2] ANSSI, "Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine." <http://www.ssi.gouv.fr/guide-dns>, May 2014.

[3] ANSSI, "Recommandations de sécurité relatives à TLS," tech. rep., 2016.

[4] ANSSI, "Comprendre et anticiper les attaques DDoS." <http://www.ssi.gouv.fr/guide-ddos>, 2015.

[5] ANSSI, "MaBo - MRT and BGP in OCaml." <https://github.com/ANSSI-FR/mabo>.

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

[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." <https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-22>, 2017.

[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." <https://github.com/rvarloot/asrank>, 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." <http://www.discoproject.org/>.

[15] BGPMon, "Large hijack affects reachability of high traffic destinations." <https://bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/>, April 2016.

[16] 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, 8020.

[17] 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.

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

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

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

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

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

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

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

[25] 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.

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

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

[28] ANSSI, "Référentiel Général de Sécurité." <http://www.ssi.gouv.fr/rgs>, June 2014.

[29] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full SHA-1." <https://shattered.io/static/shattered.pdf>, Janvier 2017.

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

[31] 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, 7919.

[32] 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, 7919.

[33] 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, 7905, 7919.

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

[35] O. Levillain, "Une étude de l'écosystème TLS." <https://www.ssi.gouv.fr/uploads/2016/11/levillain-o_these_manuscrit.pdf>, Septembre 2016.

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

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

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

[39] 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.

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

[41] ANSSI, "Recommandations de sécurité relatives à TLS." <https://www.ssi.gouv.fr/nt-tls>, Août 2016.

[42] 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>.

[43] 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.

[44] O. Levillain, M. Tury, and N. Vivet, "Concerto : A Methodology Towards Reproducible Analyses of TLS Datasets." <https://eprint.iacr.org/2017/020.pdf>, Janvier 2017.

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

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

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

[48] 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.

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

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

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

[52] Microsoft, "An update to our SHA-1 deprecation roadmap." <https://blogs.windows.com/msedgedev/2016/04/29/sha1-deprecation-roadmap/>, April 2016.

[53] Google, "SHA-1 certificates in Chrome." <https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html>, November 2016.

[54] Mozilla, "Phasing Out SHA-1 on the Public Web." <https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/>, October 2016.

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

[56] Contributing Members of the UPnP Forum, "UPnP™ Device Architecture 1.1." <http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf>, Oct. 2008.

[57] Paul Vixie et Vernon Schryver, "DNS Response Rate Limiting (DNS RRL)." <http://ss.vix.su/~vixie/isc-tn-2012-1.txt>, Apr. 2012.

[58] Akamai, "akamai's [state of the internet] / security Q4 2016 report." <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf>, Jan. 2017.

[59] Agence nationale de la sécurité des systèmes d'information (ANSSI), "Recommandations pour la sécurisation des sites web." <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html>, Apr. 2013.

[60] NTP development team, "NTP Software Downloads." <http://www.ntp.org/downloads.html>.

[61] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "Simple Network Management Protocol (SNMP)." RFC 1157 (Historic), May 1990.

[62] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)." RFC 1448 (Proposed Standard), Apr. 1993. Obsoleted by RFC 1905.

[63] Y. Y. Goland, P. Leach, Y. Gu, and S. Albrigh, "Simple service discovery protocol/1.0 operating without on arbiter," *IETF INTERNET-DRAFT draft-cai-ssdp-v1-03.txt*, 1999.

[64] Jared Mauch, "OpenResolverProject." <http://openresolverproject.org/>.

[65] Jared Mauch, "OpenNTPProject.org - NTP Scanning Project." <http://openntpproject.org/>.

[66] Jared Mauch, "OpenSNMPProject.org - SNMP Scanning Project." <http://opensnmpproject.org/>.

[67] Jared Mauch, "OpenSSDPProject.org - SSDP Scanning Project." <http://openssdpproject.org/>.

[68] NTP development team, "ntpq - standard NTP query program." <http://doc.ntp.org/current-stable/ntpq.html>.

[69] NTP development team, "ntpdc - special NTP query program." <http://doc.ntp.org/current-stable/ntpdc.html>.

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
LIR	Local Internet 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.

Juillet 2017

Licence ouverte / Open Licence (Etalab v1)

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