Observatoire de la résilience de l'Internet français

François Contat, Mathieu Feuillet, Guillaume Valadon, Pierre Lorinquer, Stéphane Bortzmeyer, Samia M'timet, Mohsen Souissi

rapport.observatoire@ssi.gouv.fr

25 janvier 2013

L'Agence Nationale de la Sécurité des Systèmes d'Information

- Créée le 7 juillet 2009, l'ANSSI :
  - est l'autorité nationale en matière de défense et de sécurité des systèmes d'information ;
  - est un réservoir de compétences au profit des administrations et des organismes d'importance vitale ;
    - à terme, l'effectif sera de 360 personnes.
- Ses missions principales sont la prévention et la défense des systèmes d'information.
- L'une de ses priorités d'action est la résilience de l'Internet.

http://www.ssi.gouv.fr

La résilience ?

« La capacité de fonctionner pendant un incident
et de revenir à l'état nominal. »

Livre blanc sur la défense et la sécurité nationale

On peut notamment observer :

- la structure de l'Internet (routage & nommage)
- le trafic et les services (HTTPS, SPAM, botnets...)

L'observatoire se focalise sur la structure de l'Internet.

Quelques mots sur l'observatoire

Les motivations à l'origine de l'observatoire :

- l'Internet reste méconnu ;
- les analyses d'incidents sont rarement orientées sur la France ;
- l'étude de l'utilisation des bonnes pratiques.

Placé sous l'égide de l'ANSSI, l'observatoire vise à :

- étudier en détails la résilience de l'Internet français ;
- favoriser les échanges techniques entre acteurs de l'Internet ;
- publier ses résultats anonymisés ;
- diffuser des bonnes pratiques.

L'AFNIC est moteur de l'initiative depuis ses débuts.

Identification automatique des AS français

Le besoin

- travailler avec plus de 4 AS ;
- identifier automatiquement les AS français ;
  - via un algorithme d'apprentissage ;
- tenter d'appréhender *l'Internet français*.

Résultats

- 1270 AS français (810 sont réellement annoncés) ;
- 9 *AS* en moins que les bases du RIPE et CYMRU ;
- entre 40 et 70 en plus.

Indicateurs BGP & résultats

Indicateurs BGP

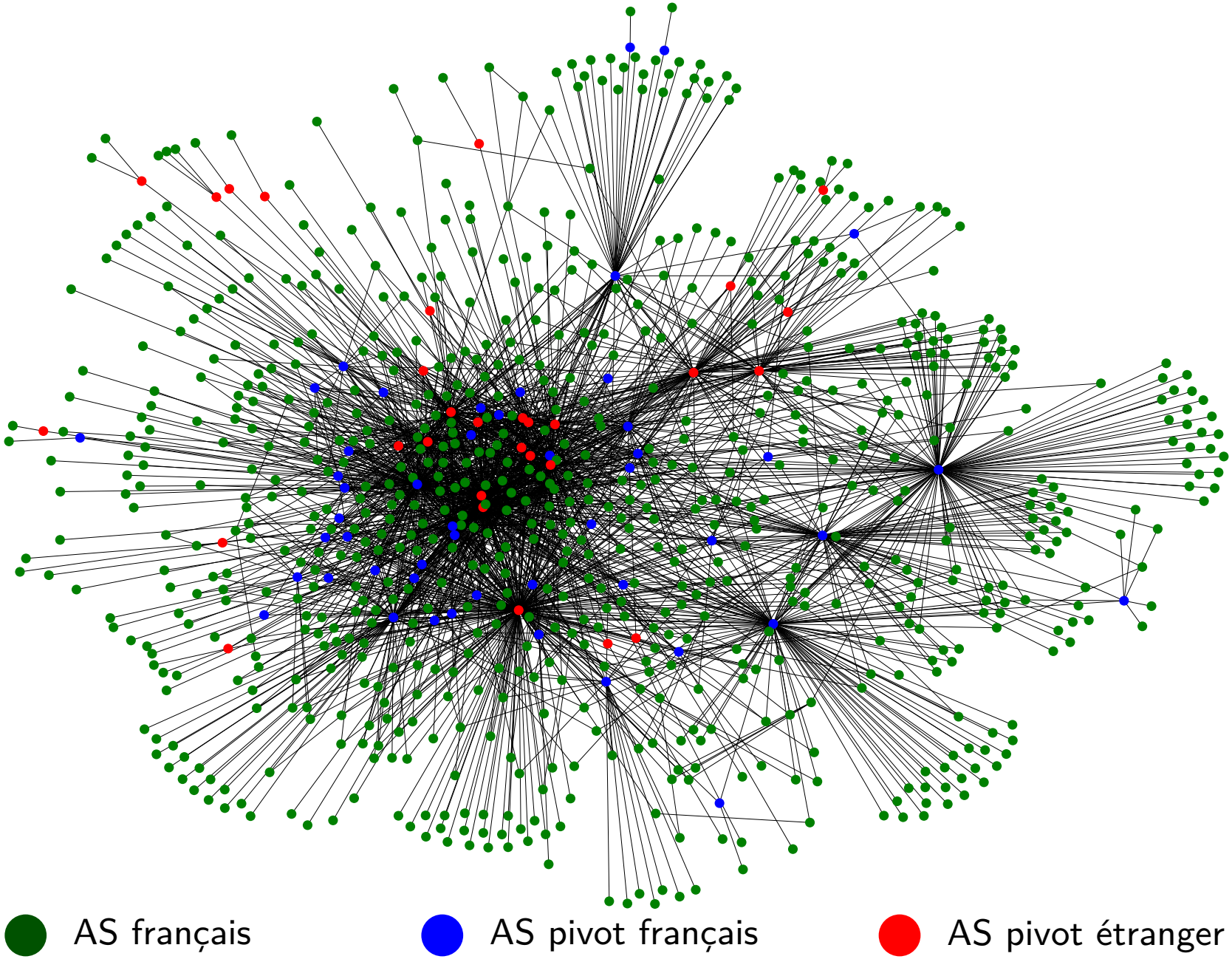
Indicateurs

- connectivité des AS (IPv4 et IPv6) ;
- usurpations de préfixes ;
- obsolescence des objets route ;
- filtrage des annonces via objets route ;
- mise en œuvre des bonnes pratiques ;

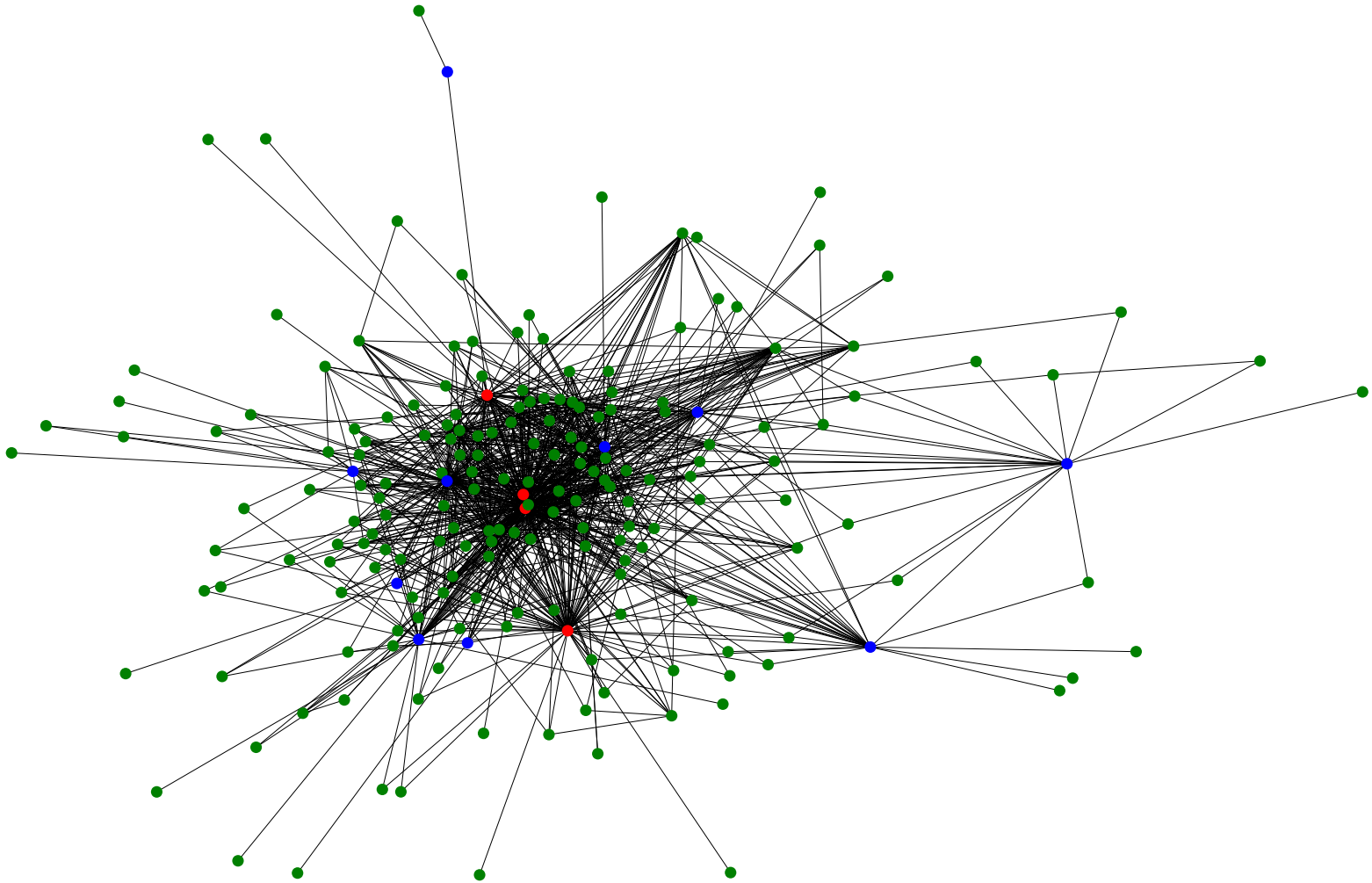
2011 analyse de quatre grands opérateurs français ;

2012 plus de 1200 *AS français* ont été identifiés.

Connectivité en IPv4



Connectivité en IPv6



AS français AS pivot français AS pivot étranger

Les usurpations de préfixes

L'événement de base : un AS annonce un préfixe plus spécifique ou égal à un préfixe annoncé par un autre AS, à un instant donné.

Données :

- dumps MRT du collecteur RIS au LINX (jusqu'au 31/12/2012) ;
- liste de 1270 AS français ;
- liste d'objets route jusqu'au 31/12/2012.

Méthodologie : les événements sont classés en catégories :

- *Valide* : un objet route permet de valider l'événement ;
- *Direct* : l'AS usurpateur est connecté à l'AS usurpé ;
- *Non-direct* : l'AS usurpé est sur le chemin ;
- *Hijack* : l'AS usurpé n'est pas sur le chemin.

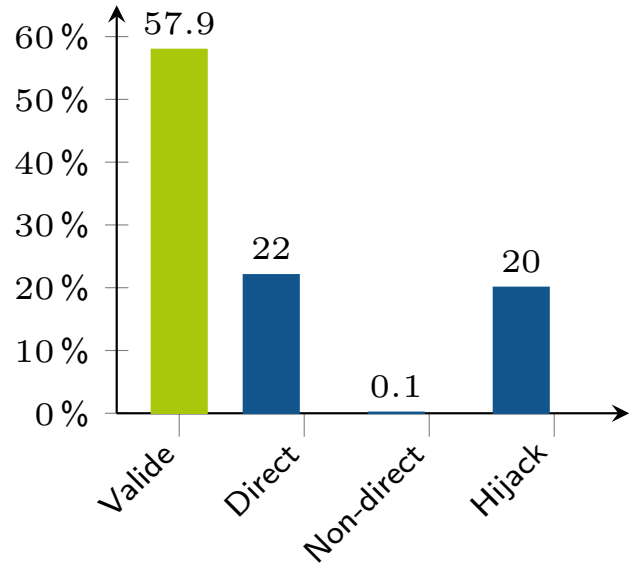
Résultats globaux

AS

77 AS ciblés par des événements :

- avec *objets route* : 42
- sans *objet route* : 35

13108 (0.22%) événements dont l'origine est un AS privé.



Nombre d'événements : 6088284
Nombre d'événements uniques : 1580

Nature des AS

- AS usurpateurs : 129 (84 sont français)
- AS laxistes : 122 (43 sont français)

Durée des usurpations

- 19 AS usurpés tous les jours ;
- 51% des événements durent moins de 2 heures.

Filtrage des annonces via objets route

Objet route : le mainteneur de l'AS déclare à son IRR les préfixes qu'il annonce.

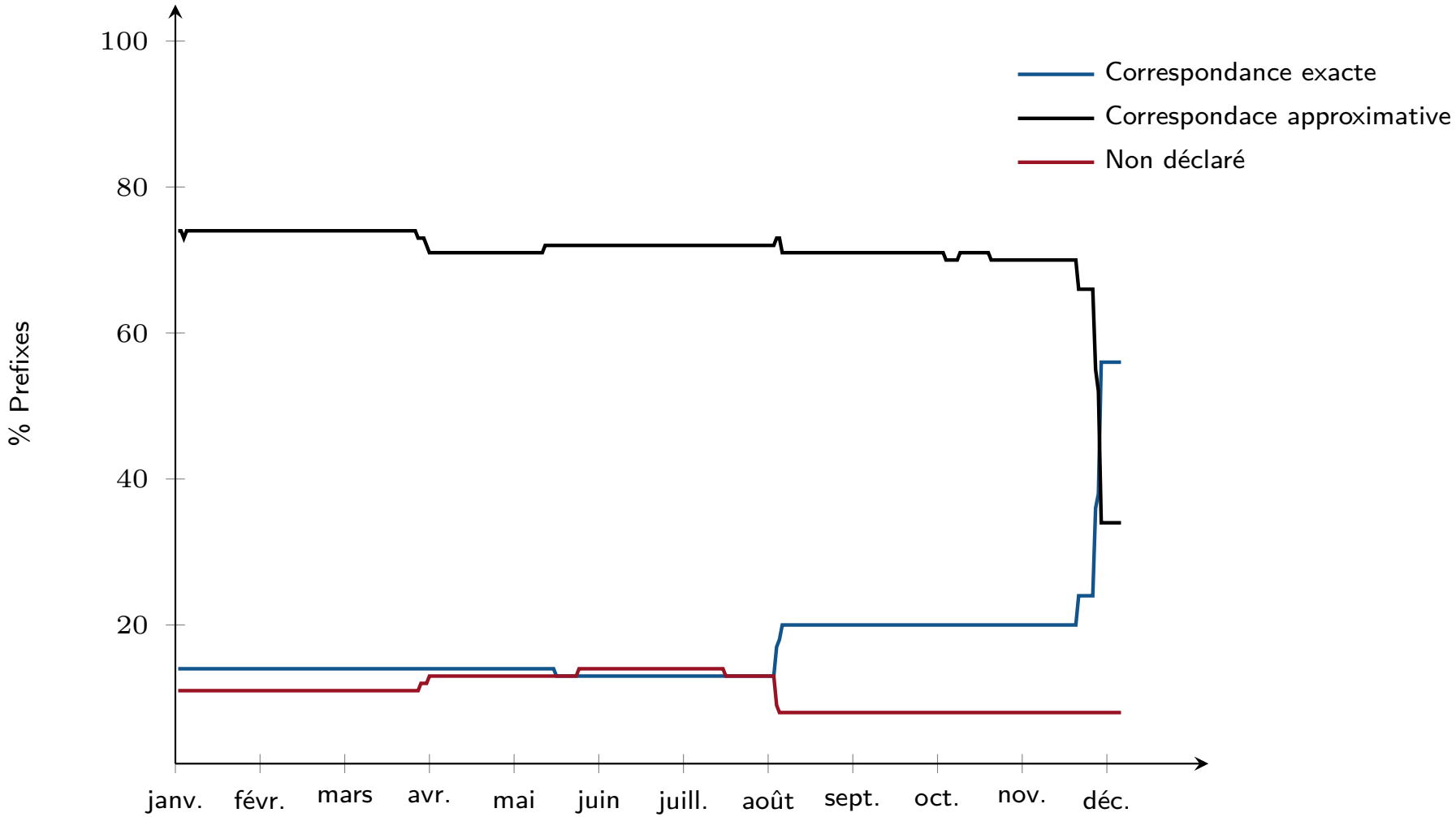
Utilité :

- aucun mécanisme de preuve d'origine des annonces dans BGP ;
- authentification du déclarant par l'IRR ;
- base de données publique de correspondance IP/AS.

Mesure de l'indicateur :

- données sources : préfixes annoncés sur Internet ;
- comparaison quotidienne des données sources avec les objets route déclarés

Filtrage des annonces via objets routes - Exemple



Obsolescence des déclarations avec l'Internet

Mesure de l'indicateur :

- données sources : dépôt quotidien du RIPE ;
- comparaison quotidienne des données sources aux préfixes annoncés vus sur le RIS.

AS	inutilisé 2011	inutilisé 2012
AS-fr1	5.3%	5.3%
AS-fr2	5.5%	0%
AS-fr3	48.4%	24%
AS-fr4	47.7%	48.6%

503 AS n'ont aucun objet route déclaré.
512 AS ont tous leurs préfixes couverts par des objets routes.

Nouveaux indicateurs - Bonnes pratiques

Taille maximum de CIDR annoncés par ou traversant des AS français avec AS_PATH > 2 :

- IPv4 : /24 (RIPE-399) $=>$ 5 préfixes annoncés sur 440 000 ;
- IPv6 : /48 (RIPE-532) $=>$ 43 préfixes annoncés sur 12 000.

AS_PATH contenant des numéros d'AS illégitimes annoncés par ou traversant des AS français :

- numéros d'AS documentation (64496-64511) ;
- numéro d'AS privé (64512-65534).

12 AS_PATHes incorrects recensés sur l'année 2012 (8 sur le long de l'année)

Indicateurs DNS & résultats

Les indicateurs DNS (Édition 2011)

- Dispersion topologique des serveurs DNS faisant autorité
  - nombre de serveurs, AS et pays par zone
- Pourcentage des résolveurs vulnérables à la faille Kaminsky
  - les ports source ne sont pas "assez aléatoires"
- Pénétration de DNSSEC sous .fr
- Pénétration d'IPv6
  - pourcentage de zones sous .fr ayant des serveurs DNS/Web/-Mail compatibles IPv6
  - pourcentage de requêtes DNS transportées en IPv6 (reçues par nos serveurs)

Deux nouveaux indicateurs DNS pour l'édition 2012

- Qualité technique des zones
  - conformité des serveurs DNS faisant autorité à un ensemble de bonnes pratiques
- Résolveurs les plus demandeurs
  - Objectif : étude de la concentration des résolveurs et de la part des résolveurs individuels/FAI/publics

Plateforme/outils de mesures

DNSwitness (`http://www.dnswitness.net/`), une plateforme de mesures "maison", avec 2 composantes :

- mesures actives, DNSdelve : exploration de services/ressources par requêtes DNS sortantes ciblant des zones sous .fr
- mesures passives, sonde DNSmezzo : analyse des requêtes DNS entrantes sur des serveurs faisant autorité de .fr

Mesure des indicateurs DNS

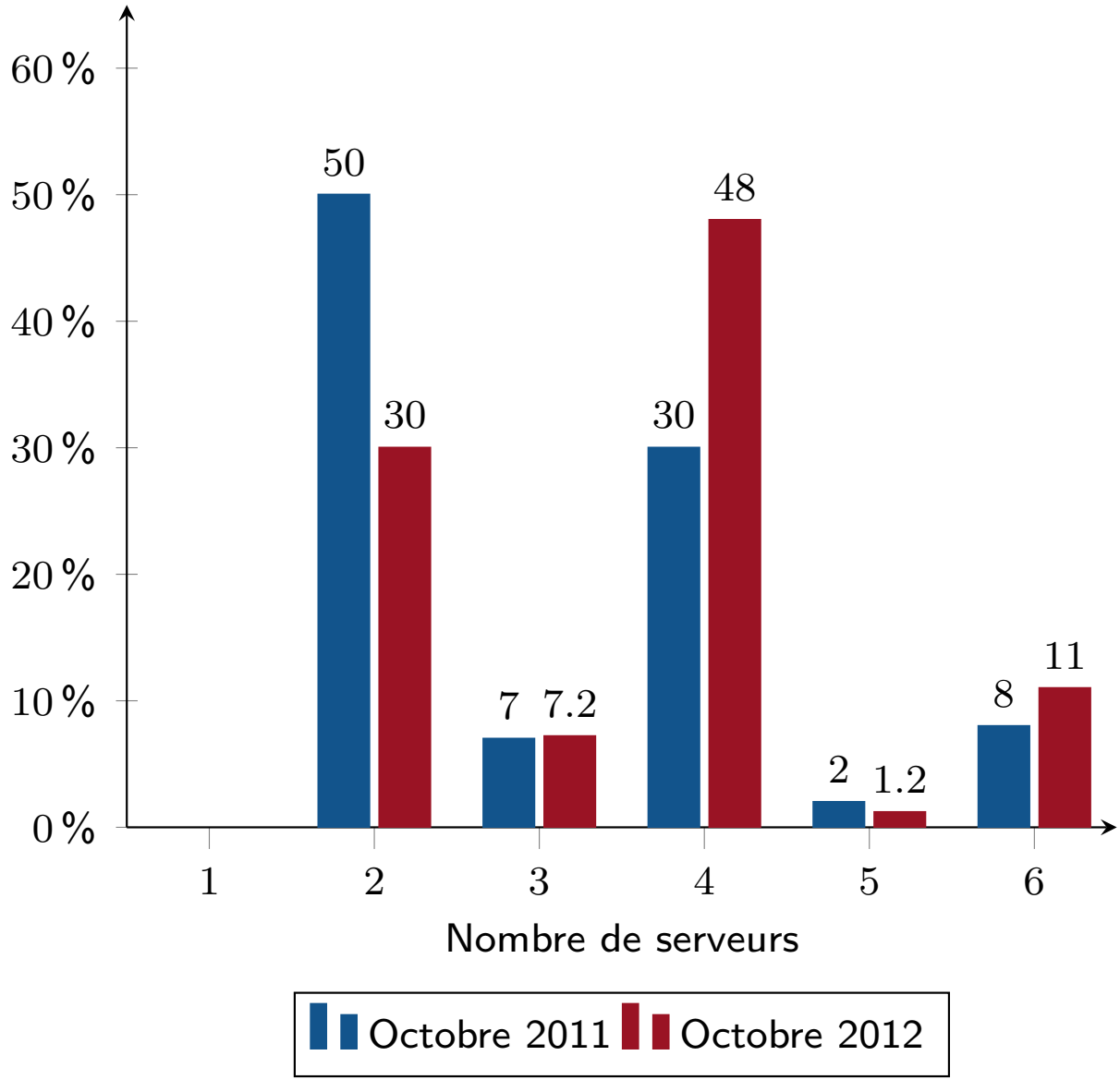
- Chaque composante (dnsdelve, dnsmezzo) comprend plusieurs modules pour mesurer l'ensembles des indicateurs
- Exemple pour l'indicateur de pénétration d'IPv6 :
  - module IP de DNSdelve : mesure de la pénétration par la publication de AAAA pour les services DNS/Web/Mail
  - DNSmezzo : mesure de la pénétration dans le transport et du pourcentage de requêtes demandant un AAAA

Les résultats DNS

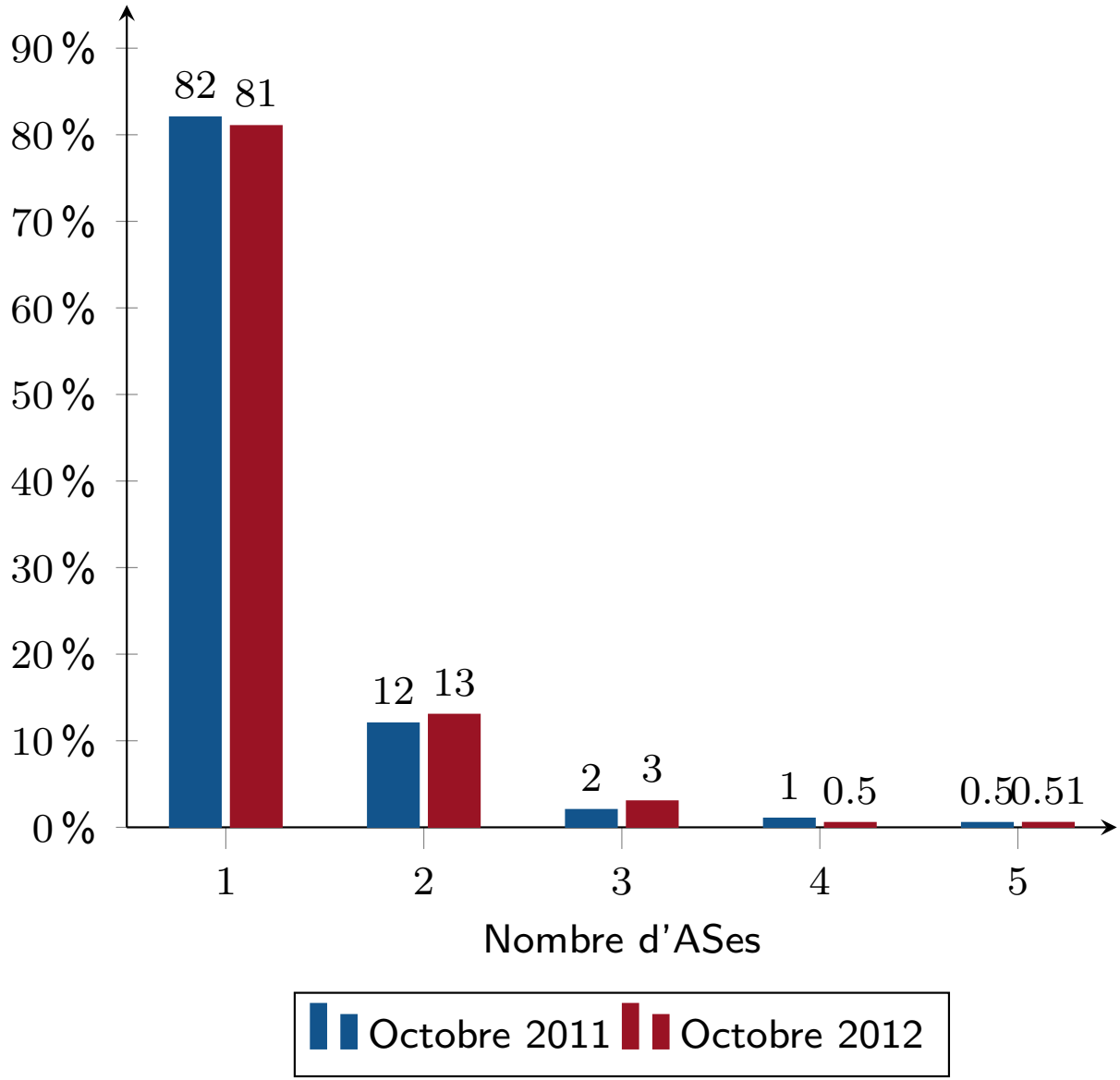
Dispersion topologique des serveurs DNS faisant autorité

1. en 2012 davantage de serveurs de noms par zone qu'en 2011 : 3,5 en moyenne
2. toujours pas assez d'AS par zone : 1,25 en moyenne ← La plus grosse faiblesse,
3. 1,2 pays par zone.

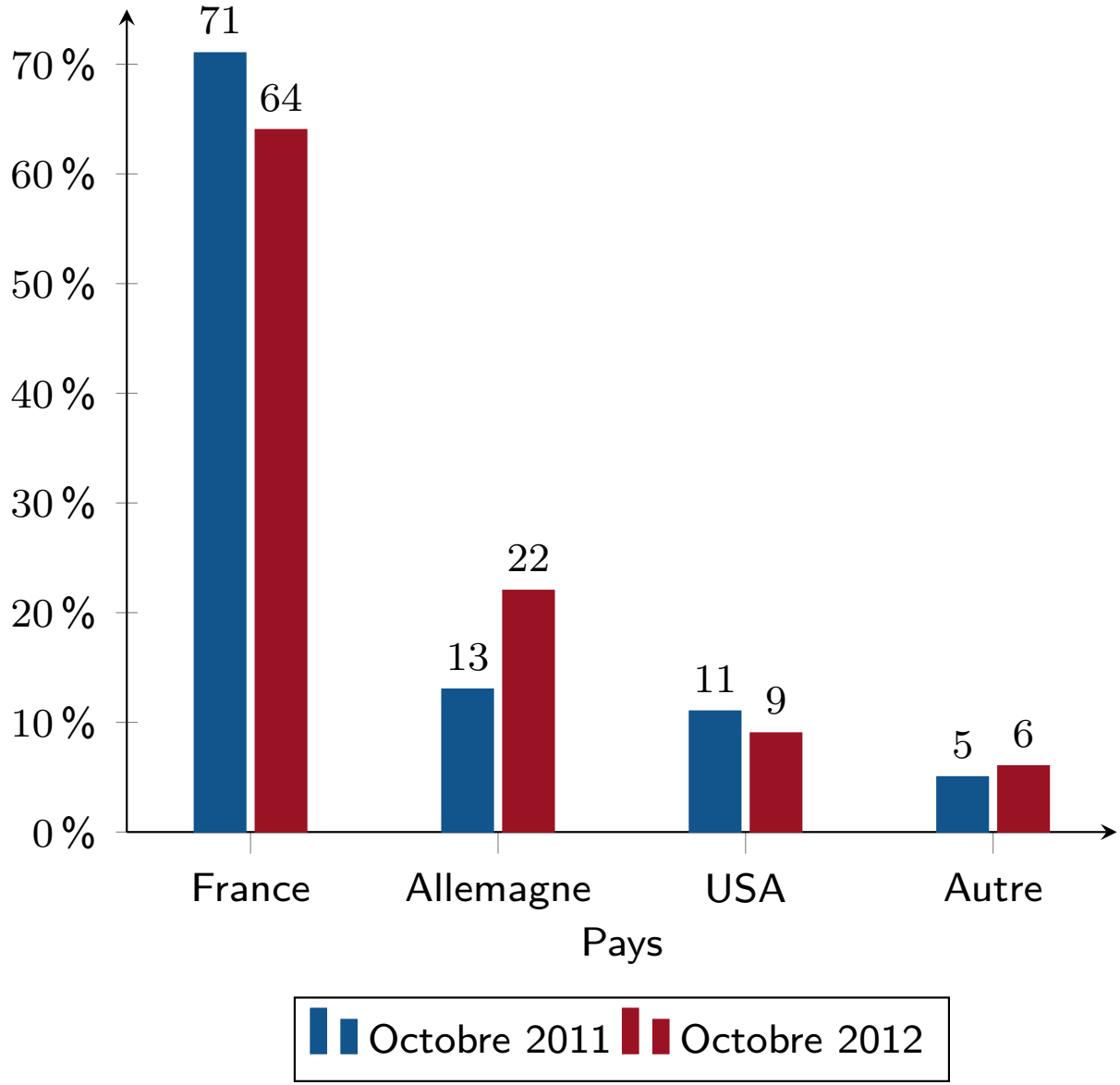
Nombre de serveurs DNS par zone



Nombre d'AS par zone



Distribution par pays



Les résultats DNS

Pourcentage des résolveurs vulnérables à la faille Kaminsky

- 4,8% des "gros" résolveurs encore vulnérables en 2012 (9% en 2011)
- Cela représente 1,4% des requêtes reçues en 2012 (5% en 2011)

Pénétration de DNSSEC sous .fr

- 35.000 zones avec DNSKEY en 2012 (170 en 2011)
- 33.790 zones avec DS dans la zone .fr en 2012
- la majorité des zones signées hébergées chez un seul hébergeur DNS

Les résultats DNS

Pénétration IPv6

- nette progression des serveurs DNS IPv6 (40% en 2011, 60% en 2012)
- stagnation des serveurs mail (10% en 2012) et mail (3,5% en 2012)
- progression des requêtes avec transport IPv6 (3% en 2011, 9% en 2012)
- stagnation des requêtes AAAA (11% en 2012)

Les résultats DNS

Deux nouveaux indicateurs pour l'édition 2012 : données en cours de traitement

- qualité technique des zones
- résolveurs les plus demandeurs

Conclusion

La première année et demie d'activité

- énoncer les bases de l'étude de la résilience de l'Internet ;
- développer et tester des outils ;
- identifier puis mesurer des indicateurs représentatifs ;
- tenter de caractériser l'*Internet français* ;
- amorcer les discussions relatives à la résilience.

Les résultats

- premier rapport rédigé par l'ANSSI et l'AFNIC ;
  - disponible en ligne sur les sites de l'ANSSI et de l'AFNIC ;
  - le second rapport est en cours de rédaction.
- rédaction d'un guide de bonnes pratiques BGP.

Conclusion du rapport 2011

1. recommandations concernant les protocoles BGP et DNS :
   - déclaration systématique et cohérente des *objets route* ;
   - plus grande dispersion des serveurs DNS faisant autorité.
2. les déploiements d'IPv6 sont peu nombreux :
   - pas de changement notable en 2011 ;
   - question de la qualité des implémentations ;
   - appel à la vigilance face à la facilité qu'apporte le NAT64.

La situation est aujourd'hui acceptable, mais rien ne garantit que cela suffise à l'avenir.

Perspectives pour l'Observatoire

1. diffuser des bonnes pratiques de déploiement BGP ;
2. effectuer des collectes BGP et DNS axées sur la France ;
   - BGP : appairage à un collecteur du RIS ou à celui de l'Observatoire ;
   - DNS : déploiement de DNSmezzo chez les opérateurs.
3. fournir des rapports ciblés par acteur de l'Internet.

Questions ?

Annexes

Identification automatique des AS français

Méthodologie

1. définition de critères indépendants caractéristiques du pays :
   - la description au RIPE contient des mots clés français ;
   - 75% des adresses IP sont localisées en France par *geoip* ;
   - l'organisation gérant l'AS a une adresse postale en France au RIPE ;
   - les administrateurs de l'AS ont une adresse postale en France au RIPE ;
   - c'est l'un des 32 AS unanimement français ;
   - c'est un voisin d'un de ces 32 AS ;
   - son numéro d'AS a été attribué par le RIPE.
2. étiquetage des AS par critères : français, étranger, inconnu ;
3. classification automatique (algorithme des k-moyennes).

Durées des usurpations