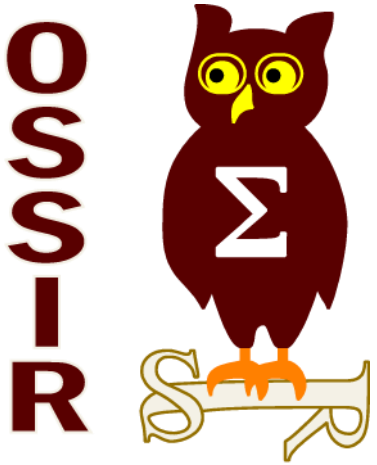


Retour sur le SSTIC (en 15 minutes)

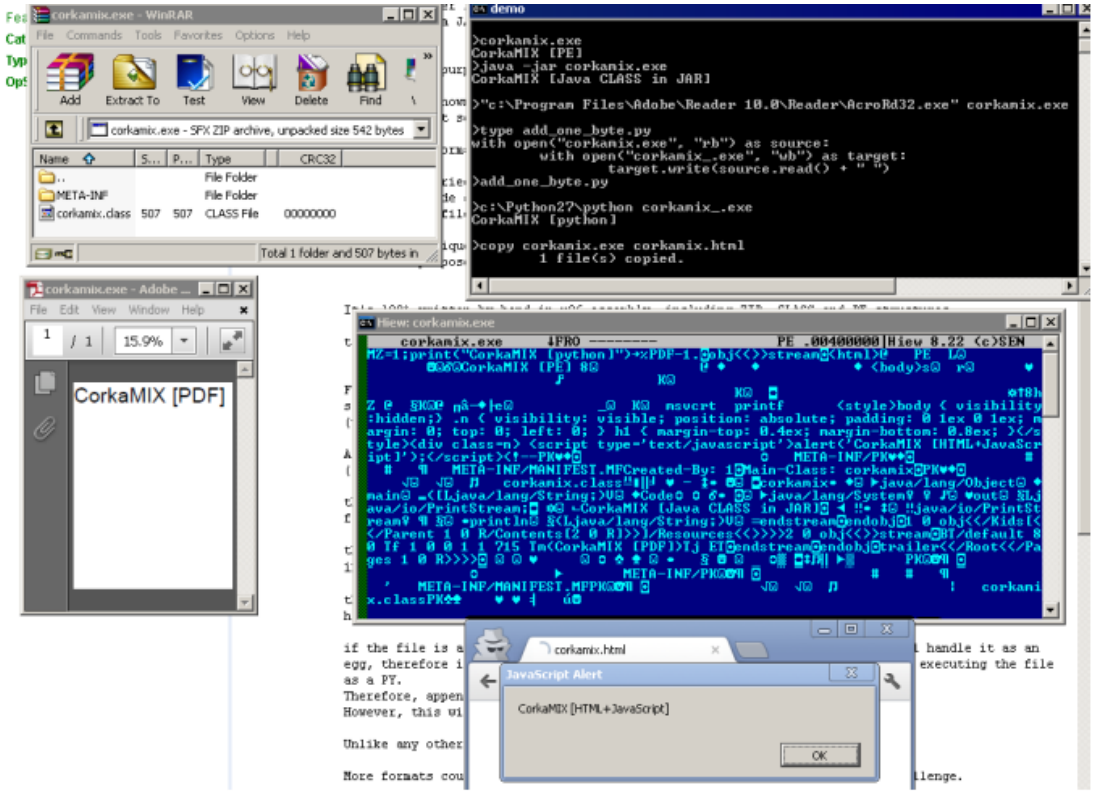
OSSIR Résist – Septembre 2013

Presented by
Etienne Maynier

MDAL
WE PROTECT YOUR ASSETS

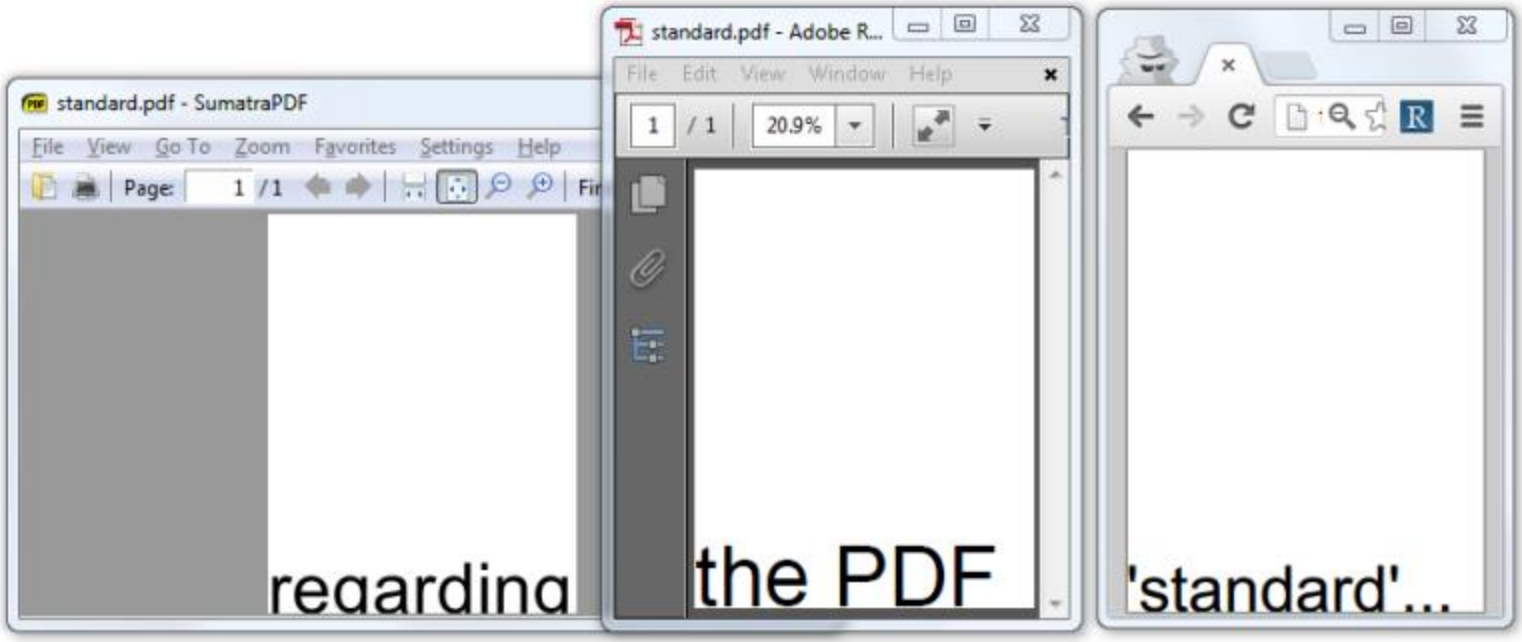
Polyglottes binaires et implications (1/3)

- Par Ange Albertini
- Etude des formats PE, Java, HTML, PDF et ZIP



- https://www.sstic.org/media/SSTIC2013/SSTIC-actes/polyglottes_binaires_et_implications/SSTIC2013-Article-polyglottes_binaires_et_implications-albertini.pdf

Polyglottes binaires et implications (2/3)

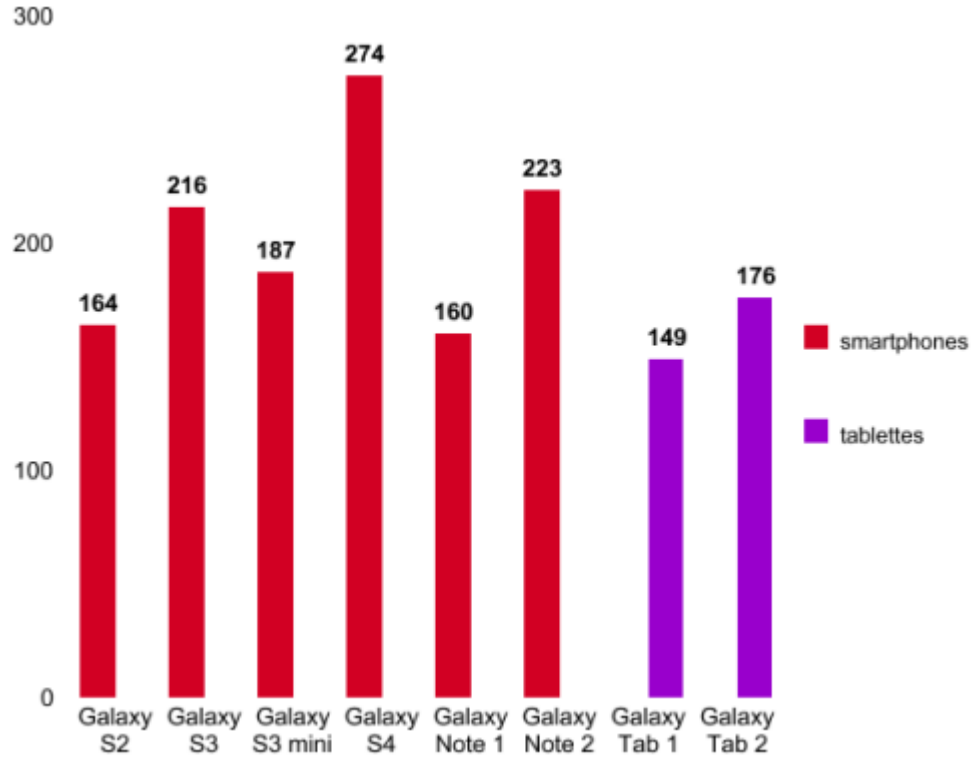


Polyglottes binaires et implications (3/3)

SHA256:	2a9c7a16cdb3c3f2285afaf61072dd5e7cc022e97f351cad6234a13e5216f389
SHA1:	e27faaa006229f8e4ab97fba7019dc9f2797f84d
MD5:	88cad2b56ab67b43794a0f7a4e690fd5
File size:	1.5 KB (1530 bytes)
File name:	corkamix.exe
File type:	PDF
Tags:	pdf

Sécurité des applications Android constructeurs (1/4)

- Par André Moulu, Quarkslab
- Travail sur les applications constructeurs du Galaxy SIII



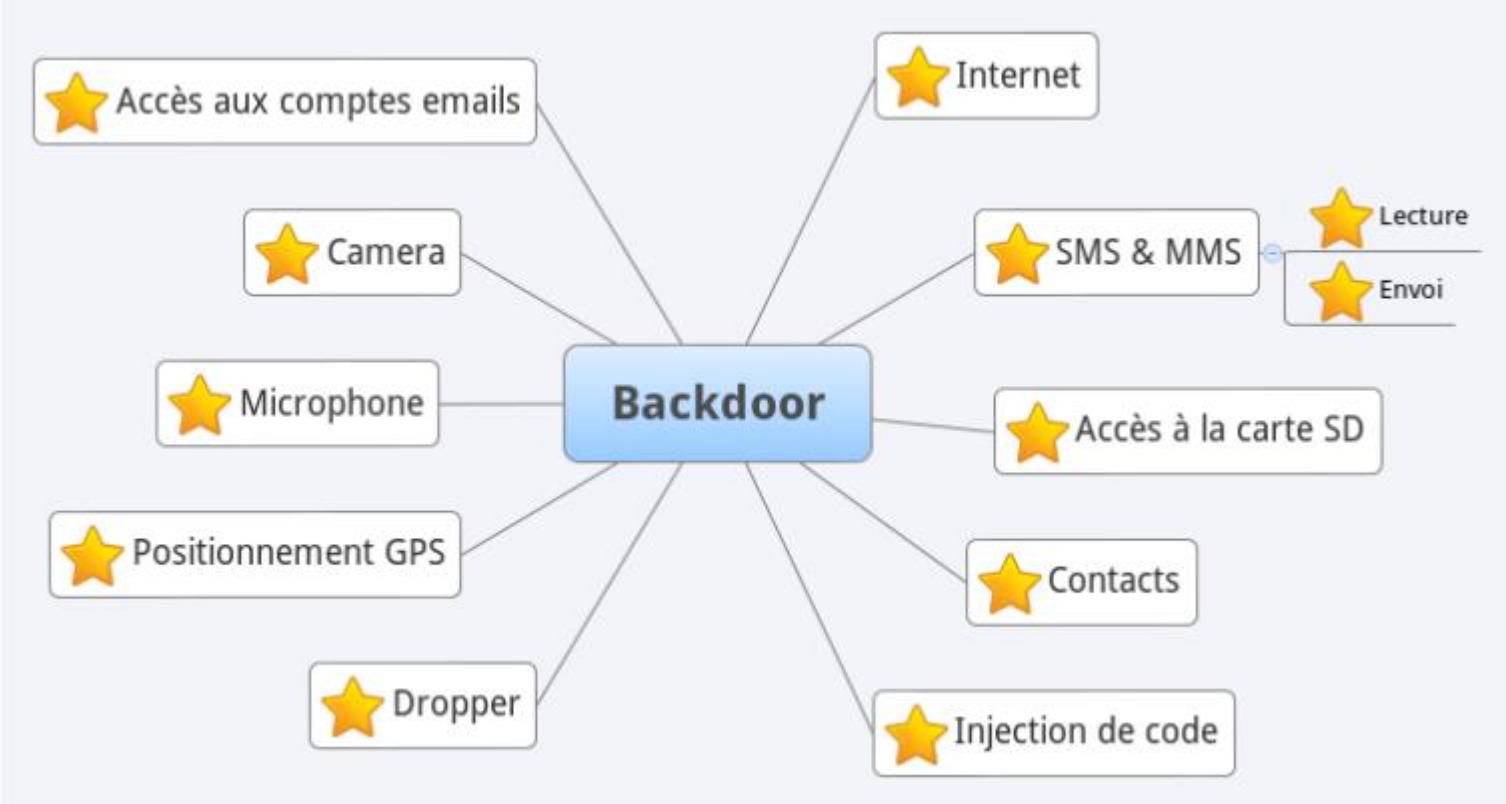
Nombre d'applications constructeur par modèle

Sécurité des applications Android constructeurs (2/4)

FTATDumpService.onStartCommand()

```
 1  public int onStartCommand(Intent paramIntent, int paramInt1, int paramInt2)
 2  {
 3    Log.i("FTATDumpService", "onStartCommand()");
 4    this.mHandler.sendEmptyMessage(1005);
 5    final String str = paramIntent.getStringExtra("FILENAME");
 6    [...]
 7    new Thread(new Runnable()
 8    {
 9      public void run()
10      {
11        FTATDumpService.this.sendMessage(
12          FTATDumpService.access$600(FTATDumpService.this),
13          FTATDumpService.this.mHandler.obtainMessage(1014)
14        );
15        if (FTATDumpService.this.DoShellCmd("dumpstate > /data/log/" + str + "
              .log"))
16          FTATDumpService.this.mHandler.sendEmptyMessage(1015);
17    [...]
18      }
19    }).start();
20    return 0;
21  }
```

Sécurité des applications Android constructeurs (3/4)



Sécurité des applications Android constructeurs (4/4)

- Post Exploitation: utilisation du MDM Samsung : SAmsung For Enterprise
  - Gestion des applications : backup, désinstallation
  - Gestion du téléphone : blocage du wifi, connexions VPN, mises à jour…
  - Transfer transparent de SMS

- Aucun patch de sécurité déployé par Samsung mais vulnérabilités corrigées dans les nouvelles ROM

Parsifal

- Implémentation de protocoles + analyse de données massives
  - Outil peu extensibles ou peu performants (scapy)
  - Nouveau framework en OCaml !

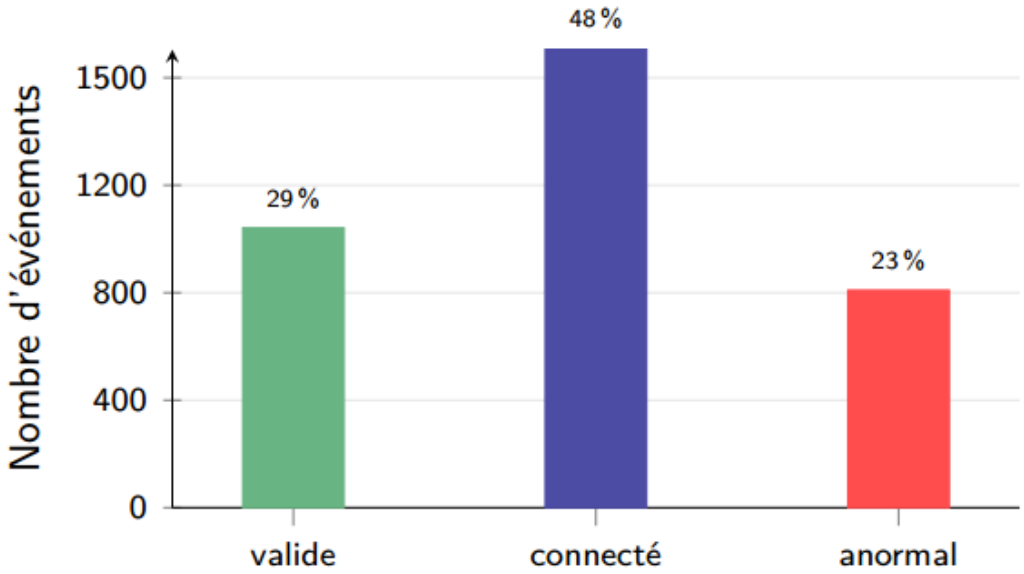
```
struct png_file = {
  png_magic : magic("\x89\x50\x4e\x47\x0d\x0a\x1a\x0a");
  png_content : binstring;
}

let input = input_of_filename "sstic.png" in
let png = parse_png_file input in
print_value (value_of_png_file png)
```

- Outil opensource par l'ANSSI!
- https://github.com/ANSSI-FR/parsifal

Observatoire de l'Internet français (1/5)

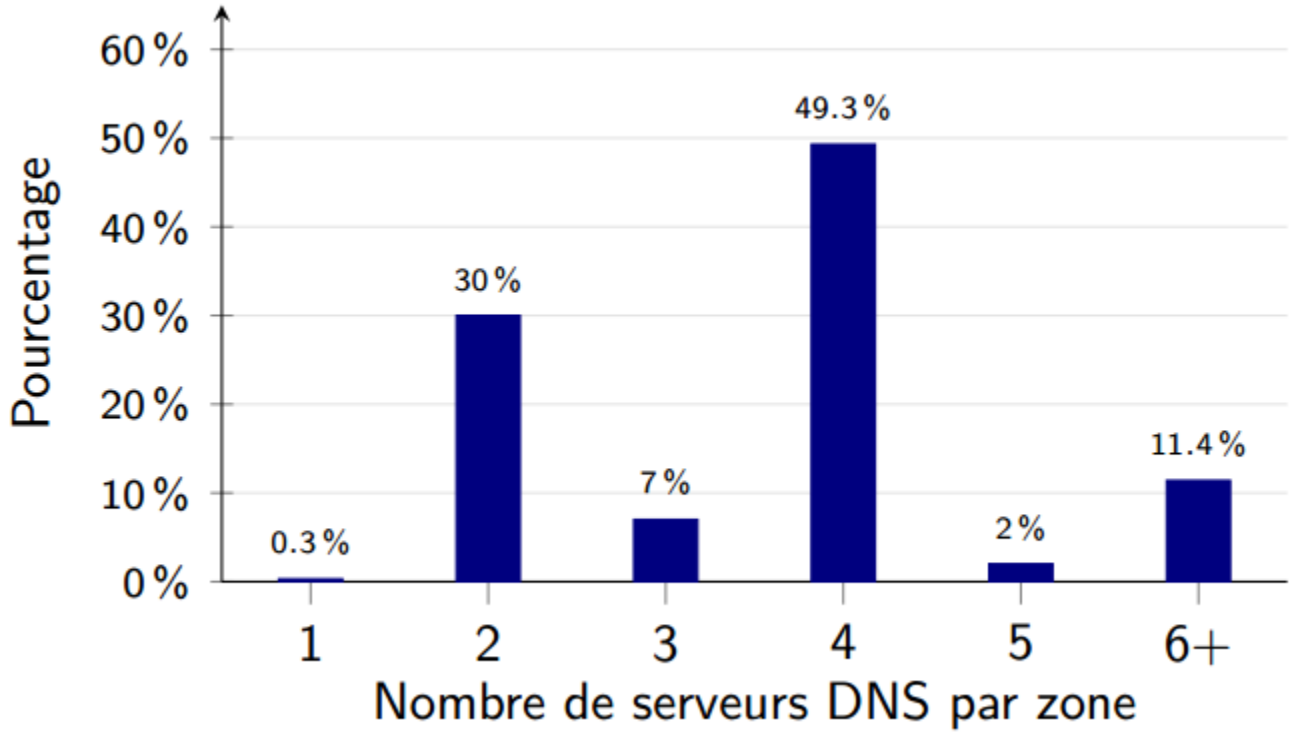
- Observation de l'Internet français
- ANSSI, AFNIC et autres acteurs français
- Surveillance de BGP et DNS



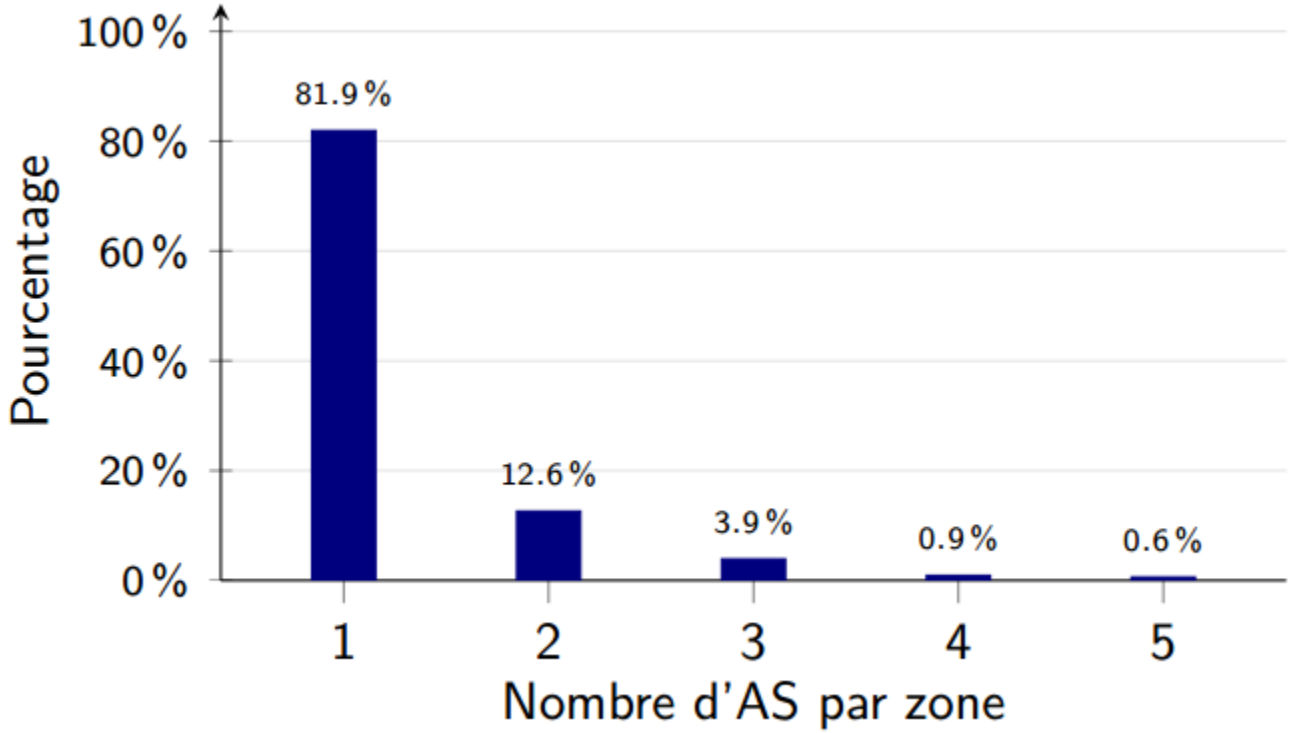
Etude des évènements BGP

Au final, seuls 7 évènements anormaux semblent être des usurpations

Observatoire de l'Internet français (2/5)

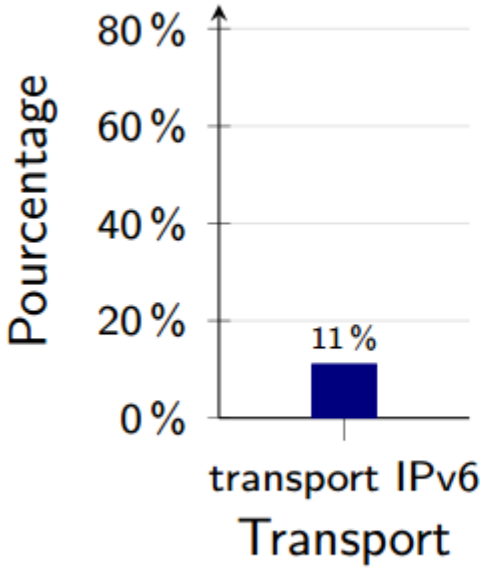


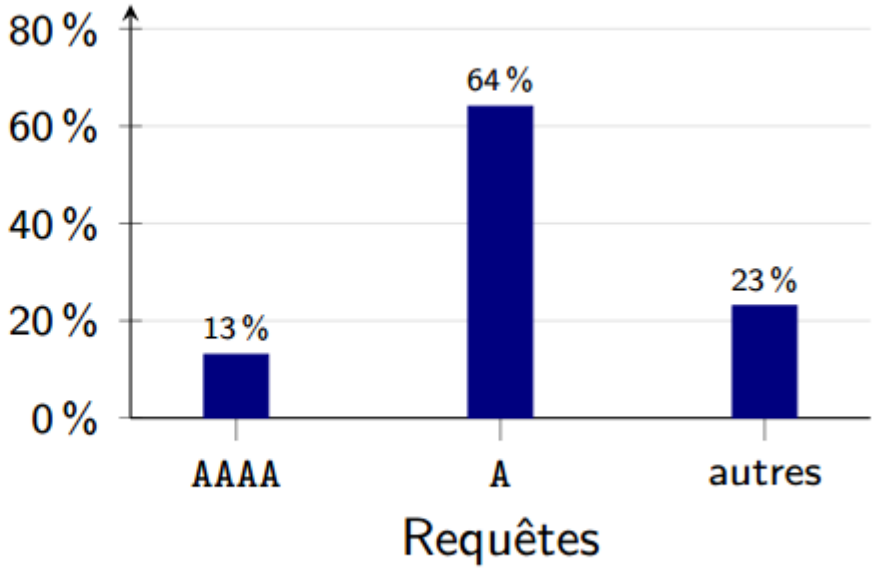
Observatoire de l'Internet français (3/5)



Observatoire de l'Internet français (4/5)

Taux de pénétration d'IPv6:





Observatoire de l'Internet français (5/5)

- « Concernant les protocoles BGP et DNS, la situation de l'Internet français est aujourd'hui acceptable, mais rien ne garantit que cela suffise à l'avenir. »

- Recommandations :
  - déployer IPv6 pour anticiper des problèmes
  - répartir les serveurs DNS faisant autorité au sein de différents opérateurs pour limiter les effets d'une panne
  - déclarer les objets route, et les maintenir à jour, afin de faciliter la détection et le filtrage d'annonces BGP illégitimes
  - appliquer les bonnes pratiques BGP au niveau des interconnexions entre opérateurs

The end

- Plus d'informations
  - https://www.sstic.org/2013/programme/
  - http://www.mdal.fr/tag/sstic/

- Et maintenant :
  - M. Stéphane Bortzmeyer - AFNIC
  - *La sécurité d'IPv6*