DNS & Vie privée

Shaft, 30 juin 2017

Shaft

Internaute auto-radicalisé

Chief Disruption Officer, Shaft Inc.

Mail : john+pses@shaftinc.fr

Mastodon : shaft@mamot.fr

Blog : https://www.shaftinc.fr/

GPG : A2C3 885D 0501 EF60

Sommaire

- Le DNS, quelques rappels
- Vous avez dit vie privée ?
- Les solutions proposées
- Conclusion

Le DNS, quelques rappels

Le DNS, quelques rappels

- Au cas où, DNS = Domain Name System

Le DNS, quelques rappels

- Au cas où, DNS = Domain Name System
- Technologie indispensable, devenue partie intégrante de l'infrastructure d'Internet

Le DNS, quelques rappels

- Au cas où, DNS = Domain Name System
- Technologie indispensable, devenue partie intégrante de l'infrastructure d'Internet
  - Invisible pour la plupart (sauf en cas de panne)
  - Presque toutes les applications (« couche 7 ») reposent sur les noms de domaines
  - Toute activité sur le net commence (le plus souvent) par des requêtes DNS

Le DNS, quelques rappels

- Protocole ancien, complexe et méconnu

Le DNS, quelques rappels

- Protocole ancien, complexe et méconnu
  - Première norme : 1983
  - Norme actuelle : 1987 (RFC 1034 & 1035)
  - Nombreuses évolutions, ajouts et corrections depuis

Le DNS, quelques rappels

- Protocole ancien, complexe et méconnu
  - Première norme : 1983
  - Norme actuelle : 1987 (RFC 1034 & 1035)
  - Nombreuses évolutions, ajouts et corrections depuis
- Le DNS dans les grandes lignes

Le DNS, quelques rappels

- Protocole ancien, complexe et méconnu
  - Première norme : 1983
  - Norme actuelle : 1987 (RFC 1034 & 1035)
  - Nombreuses évolutions, ajouts et corrections depuis
- Le DNS dans les grandes lignes
  - Base de données décentralisée et répartie
  - Sert à résoudre des noms de domaines en données

Le DNS, quelques rappels

- Nom de domaine (NDD) = Identificateur

Le DNS, quelques rappels

- Nom de domaine (NDD) = Identificateur
  - Technique : associant un NDD à des données (IP,…)
  - « Social » : porteur d'une identité (marque, patronyme…)
  - Possédant une structure arborescente
  - Stable : les IP changent, les NDD restent

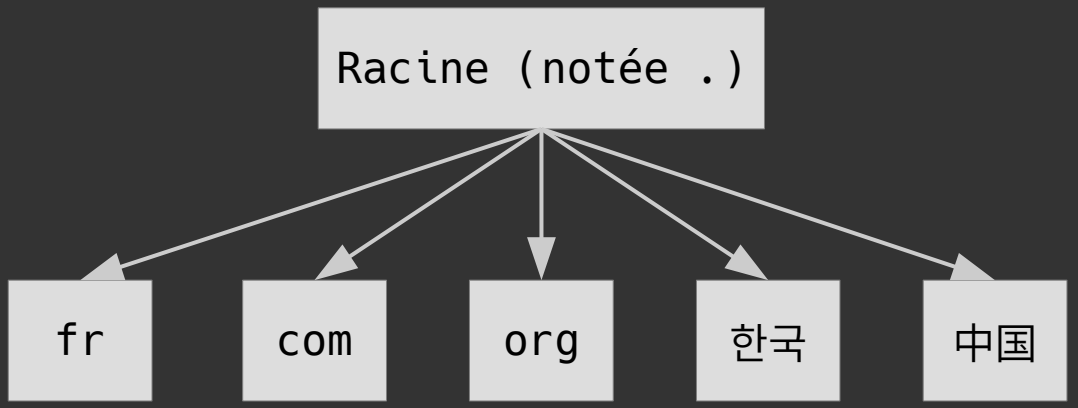
Le DNS, quelques rappels

Structure arborescente

```
Racine (notée .)
```

Le DNS, quelques rappels

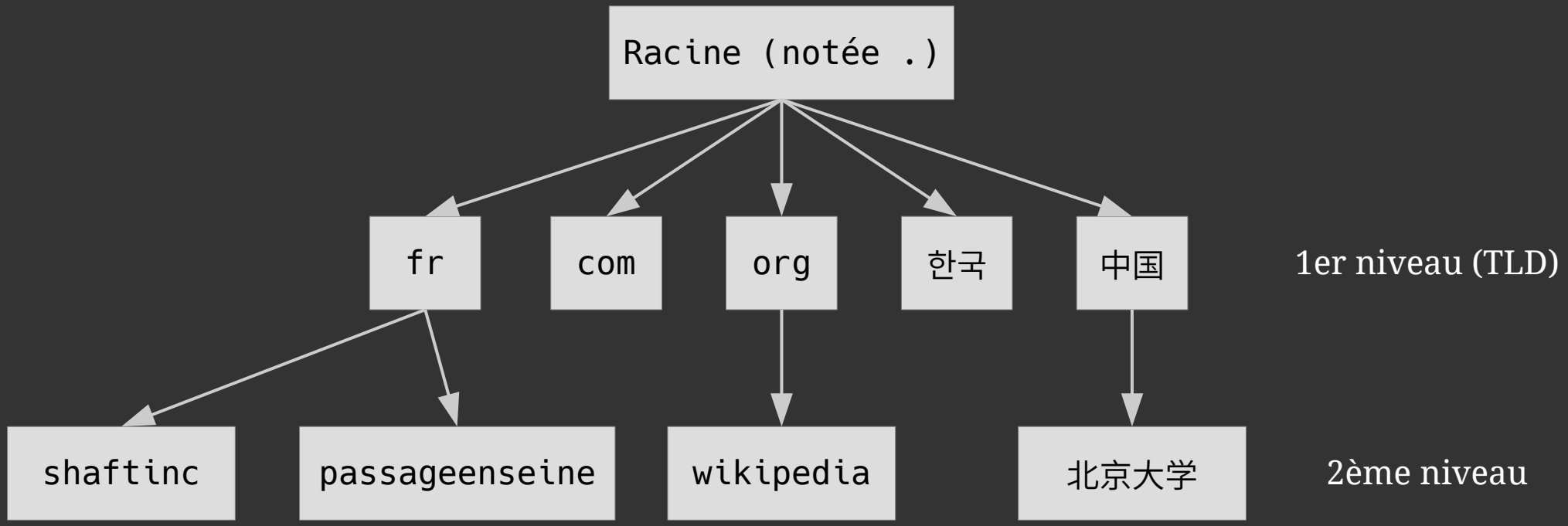
Structure arborescente



1er niveau (TLD)

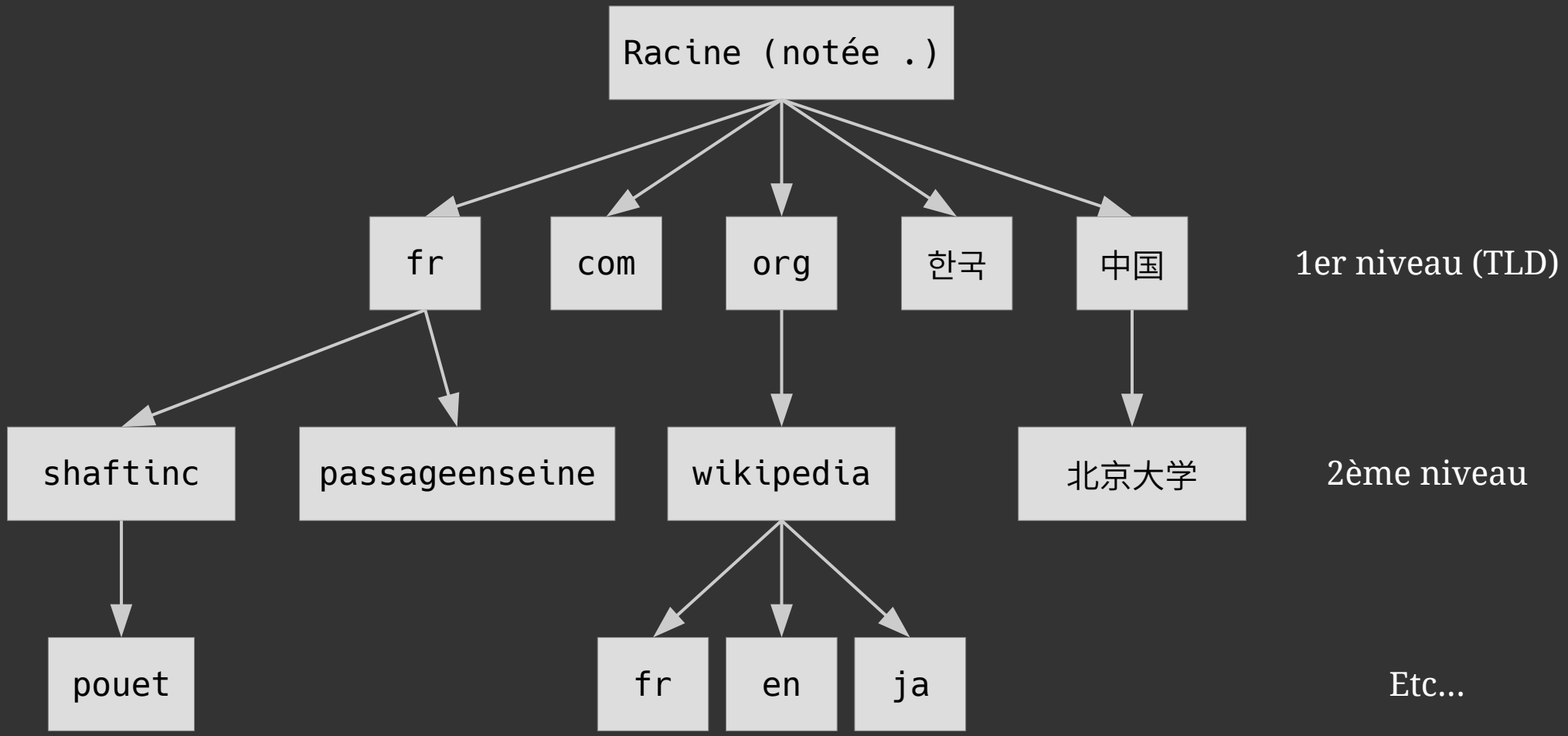
Le DNS, quelques rappels

Structure arborescente



Le DNS, quelques rappels

Structure arborescente



Le DNS, quelques rappels

A chaque NDD, on associe des données

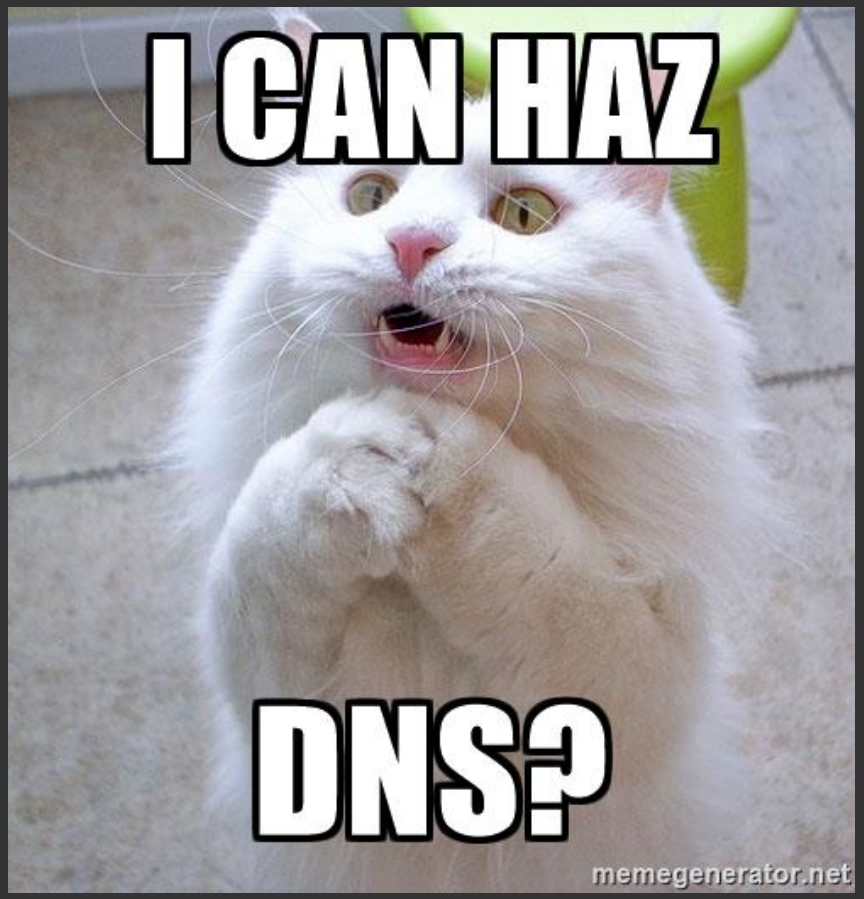
```
www.shaftinc.fr.          86400   IN      A       37.187.2.182

passageenseine.fr.        3600    IN      AAAA    2001:bc8:3f23:1000::1

assemblee-nationale.fr. 300     IN      MX      0 smtp14.assemblee-
nationale.fr.

assemblee-nationale.fr. 300     IN      A       89.185.59.149

20120113._domainkey.gmail.com. 300 IN   TXT     "k=rsa\; p=MIIBIjANBgkqhki…

fr.                       172800  IN      NS      d.nic.fr.

_xmpp-client._tcp.fdn.fr. 86400 IN      SRV     5 0 5222 jabber.fdn.fr.

28182f0a278161989f90f090dabd6cab331663d8509ddbae617bb1e7._openpgpkey.bortzmey
er.org. 86400 IN OPENPGPKEY mQINBFL2VNAB…
```

Le DNS, quelques rappels

Bon et en pratique, comment ça marche ?

Le DNS, quelques rappels

Bon et en pratique, comment ça marche ?



Le DNS, quelques rappels

- Un peu de vocabulaire (RFC 7719)

Le DNS, quelques rappels

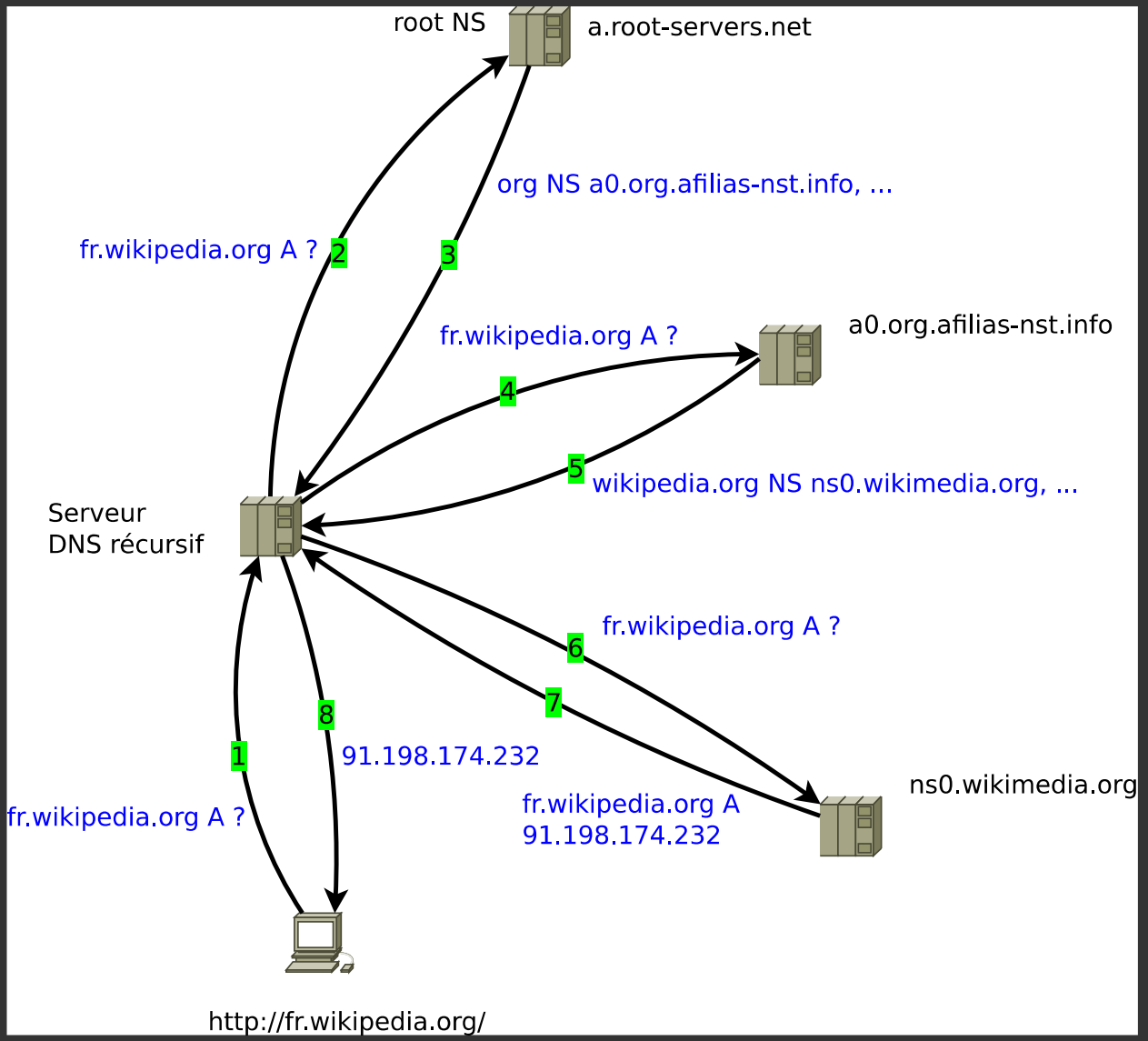
- Un peu de vocabulaire (RFC 7719)
  - **Serveur (faisant) autorité** : serveur DNS connaissant les données d'une zone grâce à un savoir local (fichier, base de données…). `l.root-servers.net` fait autorité pour la racine, `d.nic.fr` fait autorité pour `fr`, `dns104.ovh.net` pour `shaftinc.fr`.

Le DNS, quelques rappels

- Un peu de vocabulaire (RFC 7719)
  - **Serveur (faisant) autorité** : serveur DNS connaissant les données d'une zone grâce à un savoir local (fichier, base de données…). `l.root-servers.net` fait autorité pour la racine, `d.nic.fr` fait autorité pour `fr`, `dns104.ovh.net` pour `shaftinc.fr`.
  - **Résolveur** : client DNS capable de produire une réponse finale. Il est **complet** (ou **récursif**) s'il est capable de suivre les renvois des serveurs autorités. Ne connaît rien à la base (hormis les IP de la racine), apprends au fur et à mesure et garde en cache les réponses pour un temps donné.

Le DNS, quelques rappels

Mécanisme de résolution



Le DNS, quelques rappels

- Le trafic DNS voyage :

Le DNS, quelques rappels

- Le trafic DNS voyage :
  - Majoritairement via UDP
  - En clair, non chiffré

Vous avez dit vie privée ?

Vous avez dit vie privée ?

- Les données présentes dans le DNS sont le plus souvent publiques…

Vous avez dit vie privée ?

- Les données présentes dans le DNS sont le plus souvent publiques…
- …Mais le fait de les consulter relève de la vie privée

Vous avez dit vie privée ?

- Un utilisateur génère beaucoup de requêtes

Vous avez dit vie privée ?

- Un utilisateur génère beaucoup de requêtes
  - **Primaires** : sur le Web, le nom du site visité
  - **Secondaires** : sur le Web, effectuées pour récupérer scripts, CSS, traqueurs externes au site visité ou de manière « préventive » en examinant tout les liens hypertextes présent dans une page (prefetch)
  - **Tertiaires** : liées au fonctionnement du DNS (pour connaître l'IP de `passageenseine.fr` (hébergé chez Online) , il faut connaître l'adresse de `dns17.ovh.net` et donc envoyer des requêtes chez OVH

Vous avez dit vie privée ?

Florilège

```
Jun 19 19:25:51 unbound[2511:0] info: 192.0.2.18 www.shaftinc.fr. A IN
Jun 19 19:25:52 unbound[2511:2] info: 192.0.2.18 www.shaftinc.fr. AAAA IN
Jun 19 19:25:53 unbound[2511:1] info: 192.0.2.18 _443._tcp.www.shaftinc.fr. TLSA IN
Jun 19 19:25:54 unbound[2511:2] info: 192.0.2.18 download.deluge-torrent.org. A IN
Jun 19 19:26:29 unbound[2511:1] info: 192.0.2.18 router.utorrent.com. A IN
Jun 19 19:26:29 unbound[2511:2] info: 192.0.2.18 tracker.torrent.eu.org. A IN
Jun 19 19:26:31 unbound[2511:2] info: 192.0.2.18 tracker.publicbt.com. A IN
Jun 19 19:26:32 unbound[2511:2] info: 192.0.2.18 open.demonii.com. A IN
Jun 19 19:26:32 unbound[2511:3] info: 192.0.2.18 tracker.ccc.de. A IN
Jun 19 19:27:59 unbound[2511:3] info: 203.0.113.190 protonmail.com. MX IN
Jun 19 19:27:59 unbound[2511:0] info: 203.0.113.190 mail.protonmail.ch. A IN
Jun 19 19:27:59 unbound[2511:3] info: 203.0.113.190 _25._tcp.mail.protonmail.ch. TLSA IN
Jun 19 19:35:16 unbound[2706:3] info: 192.0.2.18 lemonde.fr. A IN
Jun 19 19:35:19 unbound[2706:1] info: 192.0.2.18 i2.shared.global.fastly.net. AAAA IN
Jun 19 19:35:19 unbound[2706:1] info: 192.0.2.18 cs40441145.adn.omicroncdn.net. A IN
Jun 19 19:35:21 unbound[2706:3] info: 192.0.2.18 www.binette-et-jardin.com. A IN
```

Vous avez dit vie privée ?

Florilège, sur quelques sites de presses français

Vous avez dit vie privée ?

Florilège, sur quelques sites de presses français

- Le Monde : 50 requêtes (dont `www.binette-et-jardin.com`.)
- Le Figaro : 55 requêtes
- Libération : 95 requêtes
- Le Parisien : 170 (!) requêtes

Vous avez dit vie privée ?

- Le résolveur voit (presque) tout le trafic DNS

Vous avez dit vie privée ?

- Le résolveur voit (presque) tout le trafic DNS
  - Et peut l'enregistrer (voir CGU Google Public DNS ou Cisco OpenDNS)
  - Possible d'inclure des éléments d'identifications dans les requêtes (adresse MAC,…)

Vous avez dit vie privée ?

- Le résolveur voit (presque) tout le trafic DNS
  - Et peut l'enregistrer (voir CGU Google Public DNS ou Cisco OpenDNS)
  - Possible d'inclure des éléments d'identifications dans les requêtes (adresse MAC,…)
- Tout attaquant entre l'utilisateur et le résolveur peut (facilement) écouter ce trafic

Vous avez dit vie privée ?

- Le résolveur voit (presque) tout le trafic DNS
  - Et peut l'enregistrer (voir CGU Google Public DNS ou Cisco OpenDNS)
  - Possible d'inclure des éléments d'identifications dans les requêtes (adresse MAC,…)
- Tout attaquant entre l'utilisateur et le résolveur peut (facilement) écouter ce trafic
  - Sans chiffrement, l'écoute passive est open bar
  - (programme MORECOWBELL de la NSA entre autre)

Vous avez dit vie privée ?

- Et en hébergeant son propre résolveur ?

Vous avez dit vie privée ?

- Et en hébergeant son propre résolveur ?
  - Déplace le problème vers les serveurs faisant autorité
  - En en mettant partout (nature arborescente des NDD)
  - Chaque acteur voyant par défaut la question complète
  - Un des avantages est l'utilisation du cache du résolveur
  - Mais les TTL très court (souvent ≤ 60s) utilisés sur (trop) de domaines empêchent de réellement en profiter

Vous avez dit vie privée ?

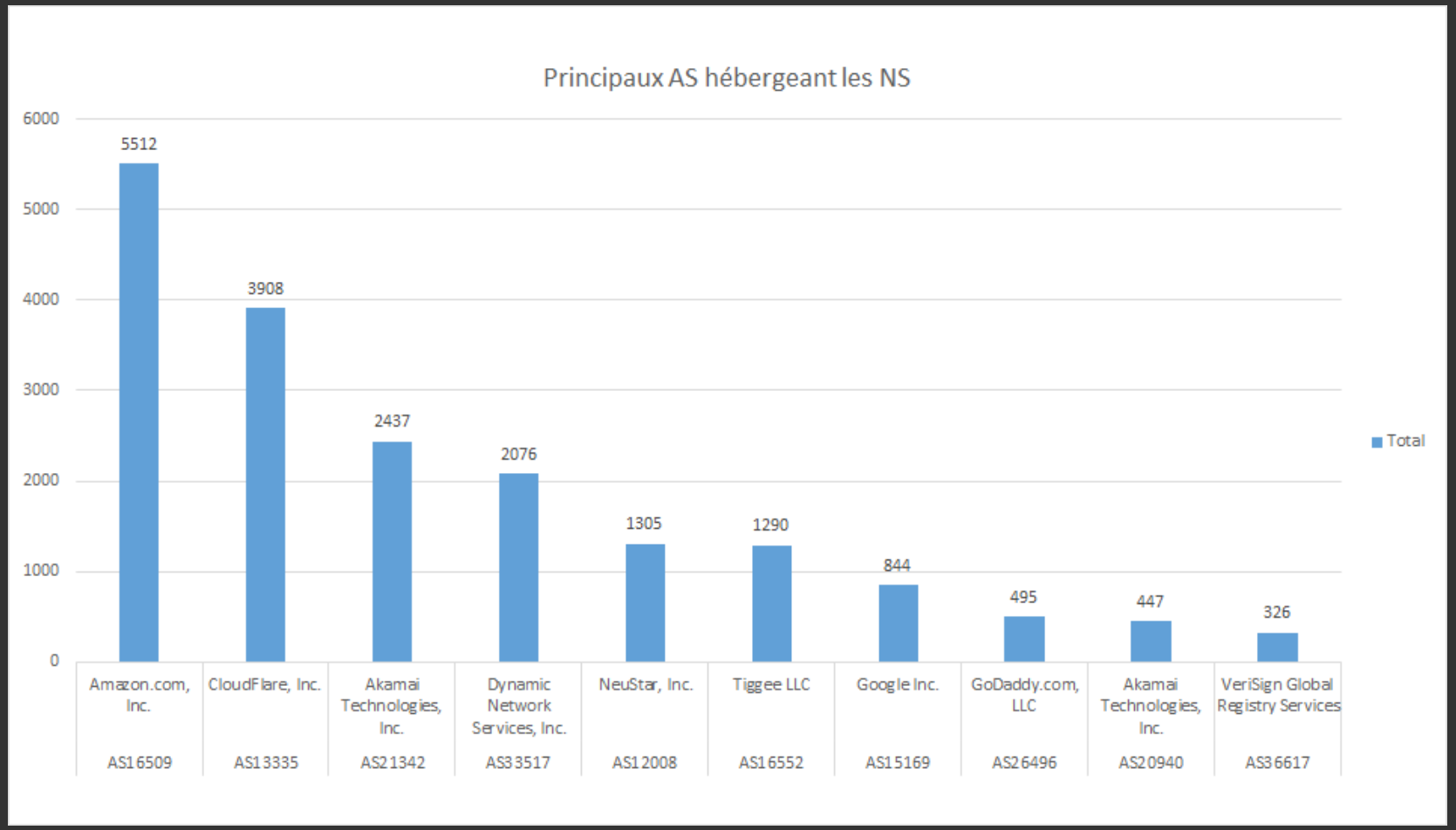
- Très forte concentration des serveurs autorités

Vous avez dit vie privée ?

- Très forte concentration des serveurs autorités
  - Beaucoup de domaines délèguent la gestion de ces serveurs
  - En 10/2016, 55 % des serveurs autorités du Top 10k Alexa étaient contrôlés par 10 prestataires (https://www.shaftinc.fr/dns-parent-pauvre.html)
  - Certains prestataires se spécialisent dans la récolte de données (Observatoire des Marques, Nameshield, MarkMonitor)

Vous avez dit vie privée ?

Centralisation mon amie (Top 10k Alexa, pour 33721 enregistrement NS)



Vous avez dit vie privée ?

WTF !?

```
# dig NS elysee.fr
(…)
;; ANSWER SECTION:
elysee.fr.              3537    IN      NS      ns2.observatoiredesmarques.fr.
elysee.fr.              3537    IN      NS      b.ns.developpement-durable.gouv.fr.
elysee.fr.              3537    IN      NS      ns3.nameshield.net.
elysee.fr.              3537    IN      NS      a.ns.developpement-durable.gouv.fr.
```

Vous avez dit vie privée ?

- En vrac

Vous avez dit vie privée ?

- En vrac
  - Il est possible de ré-identifier un internaute via le trafic DNS que sa navigation Web génère
  - Plein d’attaques possibles (détournement du serveur DHCP du routeur pour fournir un résolveur contrôlé par un attaquant, détournement du routage vers un résolveur – déjà fait en Turquie pour les résolveurs publics Google)
  - …

Les solutions proposées

Les solutions proposées

- Pas de solutions clefs en mains…
- … Mais des choses déjà existantes
- Et des travaux en cours (RFC 7626 pour documenter le problème, groupe DPRIVE à l'IETF…)

Les solutions proposées

- Chiffrer le trafic entre internaute et résolveur

Les solutions proposées

- Chiffrer le trafic entre internaute et résolveur
  - DNSCrypt (pas normalisé, implémenté dans Unbound entre autre, supporté par Cisco OpenDNS)
  - DNS sur DTLS (RFC 8094 – Expérimental, pas d’implémentation connue)
  - DNS sur TLS (RFC 7858)

Les solutions proposées

- DNS sur TLS

Les solutions proposées

- DNS sur TLS
  - Technique la plus prometteuse (TLS est bien connu)
  - Fonctionne déjà sur de nombreux résolveurs

Les solutions proposées

- DNS sur TLS
  - Technique la plus prometteuse (TLS est bien connu)
  - Fonctionne déjà sur de nombreux résolveurs
- Encore incomplet

Les solutions proposées

- DNS sur TLS
  - Technique la plus prometteuse (TLS est bien connu)
  - Fonctionne déjà sur de nombreux résolveurs
- Encore incomplet
  - Besoin de techniques complémentaires (EDNS0 Keepalive, EDNS0 Padding…) peu répandues dans les logiciels
  - Certains éléments en cours d’élaboration (dont des méthodes d’authentification du résolveur)

Les solutions proposées

DNS sur TLS, côté résolveurs

Clients

Mode		Stub						Recursive resolver			
Software		ldns (drill)	digit	getdns (Stubby)	BIND (dig)	Go DNS	Knot (kdig)	getdns[a]	Unbound	BIND	Knot Res
TCP/TLS Features	TCP fast open[b]		✔	✔				P			✔
	Connection reuse (Q/R, Q/R, Q/R)		✔	✔	✔	✔	✔			✔	✔
	Pipelining of queries(Q,Q,Q,R,R,R)	n/a	✔	✔	✔	✔	✔			✔	✔
	Process OOOR (Q1,Q2,R2,R1)	n/a	✔	✔	✔					✔	✔
	EDNS0 Keepalive[c]			✔							
TLS Features	TLS encryption (Port 853)		✔	✔		✔	✔	✔	✔		
	TLS authentication			✔			(tick)				
	EDNS0 Padding		✔	✔			✔				

Source :
https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

Les solutions proposées

- Inconvénients de DNS sur TLS

Les solutions proposées

- Inconvénients de DNS sur TLS
  - Tout doit passer par TCP
  - Nécessite plus de ressources matérielles
  - Problèmes liés à l’authentification (j’insiste, l’Homme du Milieu rôde) : nécessite un client la supportant et un serveur donnant les infos pour le faire

Les solutions proposées

DNS sur TLS, un client fonctionnel

Les solutions proposées

DNS sur TLS, un client fonctionnel

Stubby

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby

Les solutions proposées

- Stubby

Les solutions proposées

- Stubby
  - Résolveur minimum (configuration de getdns)
  - Disponible dans les bonnes crèmeries ! (inclus dans getdns 1.1+)
  - Encore en développement

Les solutions proposées

- Stubby
  - Résolveur minimum (configuration de getdns)
  - Disponible dans les bonnes crèmeries ! (inclus dans getdns 1.1+)
  - Encore en développement
- Fonctionnement

Les solutions proposées

- Stubby
  - Résolveur minimum (configuration de getdns)
  - Disponible dans les bonnes crèmeries ! (inclus dans getdns 1.1+)
  - Encore en développement
- Fonctionnement
  - Résolveur minimum → doit se connecter à un résolveur complet
  - Authentification du résolveur complet (via SPKI)

Les solutions proposées

- Pour connecter Stubby à un résolveur complet

Les solutions proposées

- Pour connecter Stubby à un résolveur complet
  - Une liste de serveurs permettant de tester est disponible : https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers
  - Rien n’empêche de monter son propre serveur :) (⚠ Ne sert pas à grand-chose si on l’utilise seul)

Les solutions proposées

- Et si on héberge son propre résolveur ?

Les solutions proposées

- Et si on héberge son propre résolveur ?
  - Pas de chiffrement pour l'instant entre résolveur et serveur faisant autorité
  - Des discussions en cours pour utiliser DNS sur TLS
  - Pose des questions pour l'authentification
  - Chiffrer ne suffit pas

Les solutions proposées

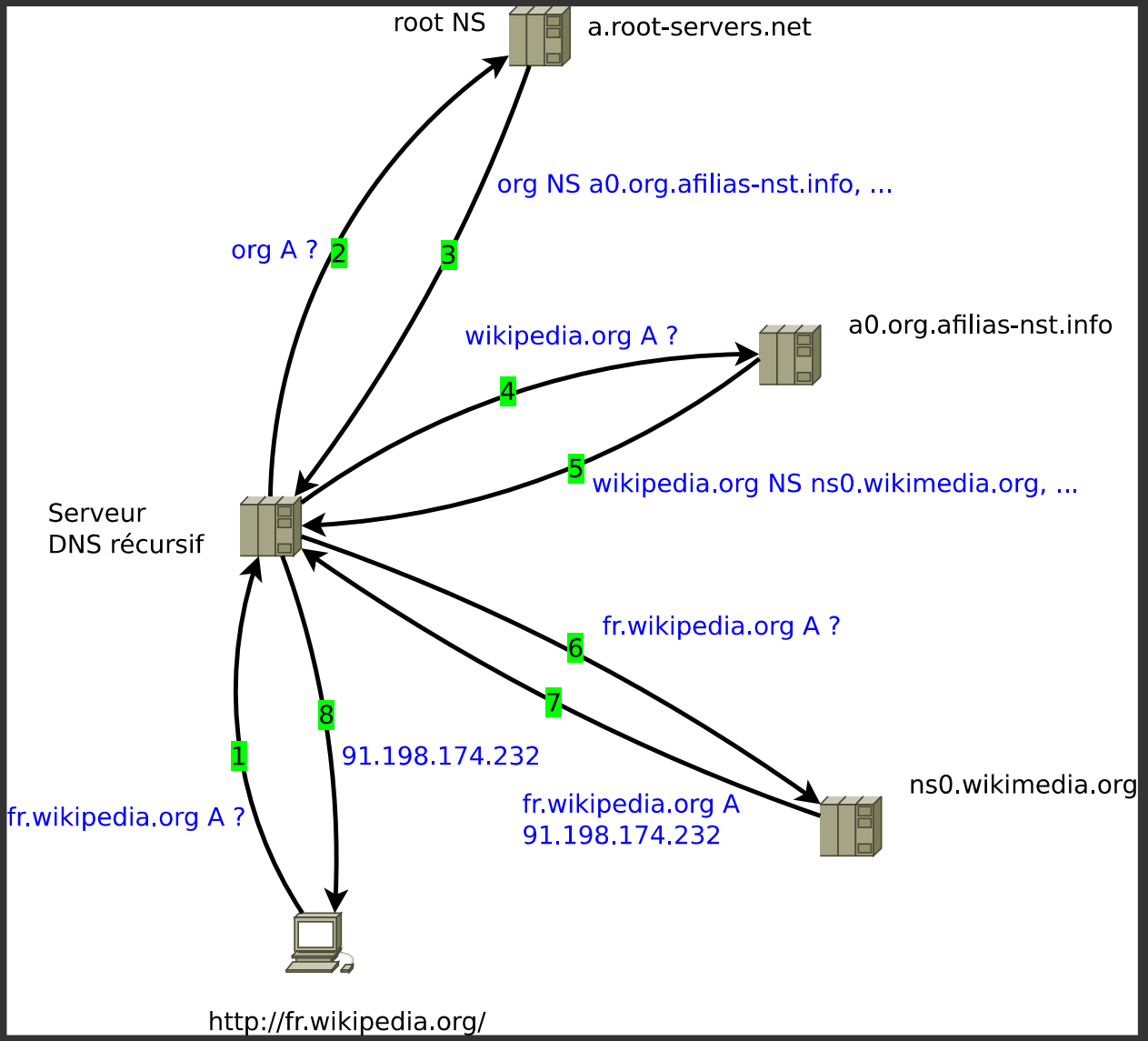
- Et si on héberge son propre résolveur ?

Les solutions proposées

- Et si on héberge son propre résolveur ?
  - Nécessité de limiter les données transmises à chaque étape de la résolution
  - QNAME Minimisation (RFC 7816)
  - Disponible notamment avec Knot Resolver (1.0.0+, activée par défaut), Unbound (1.5.7+, activée par défaut dans Debian Stretch)

Les solutions proposées

QNAME Minimisation



Les solutions proposées

- Et si on héberge son propre résolveur ?

Les solutions proposées

- Et si on héberge son propre résolveur ?
  - Il est possible de configurer son résolveur pour devenir un résolveur minimum et chiffrer la communication avec un résolveur complet
  - Pas d’authentification possible pour l’instant

Les solutions proposées

- Un peu d’hygiène numérique

Les solutions proposées

- Un peu d’hygiène numérique
  - Ne pas utiliser les résolveurs publics de Google, Cisco et cie
  - Limiter le nombre de requêtes secondaires (via résolveur menteur par exemple)
  - Passer par Tor si besoin d’anonymat
  - …

Conclusion

Conclusion

- Problème complexe… mais pas insurmontable

Conclusion

- Problème complexe… mais pas insurmontable
- Les solutions seront-elles déployées ?
  - Si HTTPS devient la norme sur le Web, c’est qu’il est poussé par de grands acteurs (Google notamment).
- Les solutions développées ne protègent pas des opérateurs indélicats
  - Le résolveur que vous utilisez voit toujours passer tout le trafic
- Développer un nouveau protocole ?

Conclusion

- Problème technique… et politique

Conclusion

- Problème technique… et politique
  - Aujourd’hui, le trafic DNS n’est à priori pas protégé par les lois et règlements relatifs à la vie privée (CNIL, RGPD…)
  - A terme, il faut l’inclure explicitement et le considérer comme une donnée personnelle

Conclusion

Merci de votre attention !

Des questions ?

Conclusion

Merci de votre attention !

Des questions ?

Conclusion

Les URLs présentées (et quelques autres)