Sécurité des noms de domaine (1/77)

Stéphane Bortzmeyer
stephane+42@bortzmeyer.org

24 janvier 2019

Plan du tutoriel

Vérifications et révisions sur la sécurité

Vérifications et révisions sur la sécurité

- Le chiffrement assure :
  1. La confidentialité
  2. L'intégrité
  3. La confiance

Vérifications et révisions sur la sécurité

- Le chiffrement assure :
  1. La confidentialité
  2. L'intégrité
  3. La confiance
- Un mot de passe se conserve :
  1. Sur un Post-It
  2. En mémoire humaine
  3. Dans un gestionnaire de mots de passe, comme Keepass
  4. Dans un coffre-fort
  5. Il ne se conserve pas, on l'oublie

Vérifications et révisions sur la sécurité, suite

Vérifications et révisions sur la sécurité, suite

- Vous recevez un courrier électronique du PDG demandant le mot de passe de l'hébergeur DNS :
  1. Vous répondez par la même voie en lui donnant la réponse
  2. Vous allez le voir et vous lui donnez en mains propres
  3. Vous refusez en indiquant l'article 6 de la Charte de Sécurité, qui spécifie le « besoin de savoir »
  4. Vous ne répondez pas, il n'a qu'à aller voir le Post-It mis sur la machine à café

Vérifications et révisions sur le DNS

Vérifications et révisions sur le DNS

- Qu'est-ce qu'un TLD ?

Vérifications et révisions sur le DNS

- Qu'est-ce qu'un TLD ?
- `http://www.elysee.fr/` est-il un nom de domaine ?

Vérifications et révisions sur le DNS

- Qu'est-ce qu'un TLD ?
- `http://www.elysee.fr/` est-il un nom de domaine ?
- Un nom de domaine, ça sert uniquement à retrouver l'adresse IP ?

Vérifications et révisions sur le DNS

- Qu'est-ce qu'un TLD ?
- `http://www.elysee.fr/` est-il un nom de domaine ?
- Un nom de domaine, ça sert uniquement à retrouver l'adresse IP ?
- `8.8.8.8` et `1.1.1.1` sont :
  1. Des serveurs DNS
  2. Des serveurs DNS de la racine
  3. Des URL
  4. Des résolveurs DNS publics
  5. Des adresses IPv4
  6. Les mots de passe du compte en banque du prof'

Le problème

Le problème

- On veut des **identificateurs**,

Le problème

- On veut des **identificateurs**,
- Idéalement, stables, lisibles, sûrs, simples, bon marché. . .

Le problème

- On veut des **identificateurs**,
- Idéalement, stables, lisibles, sûrs, simples, bon marché...
- Adaptés à l'Internet : pas de Chef ou de Directeur, et le réseau est trop gros pour tout système centralisé.

Généralités sur les noms de domaine

Généralités sur les noms de domaine

- Des noms uniques et mémorisables,

Généralités sur les noms de domaine

- Des noms uniques et mémorisables,
- Un vecteur d'identité,

Généralités sur les noms de domaine

- Des noms uniques et mémorisables,
- Un vecteur d'identité,
- Un nommage arborescent : racine, puis premier niveau, puis domaine de deuxième niveau, de troisième niveau et ainsi de suite,

Généralités sur les noms de domaine

- Des noms uniques et mémorisables,
- Un vecteur d'identité,
- Un nommage arborescent : racine, puis premier niveau, puis domaine de deuxième niveau, de troisième niveau et ainsi de suite,
- Le nombre de composants dans un nom est quelconque (2, 3, 4...)

Les noms

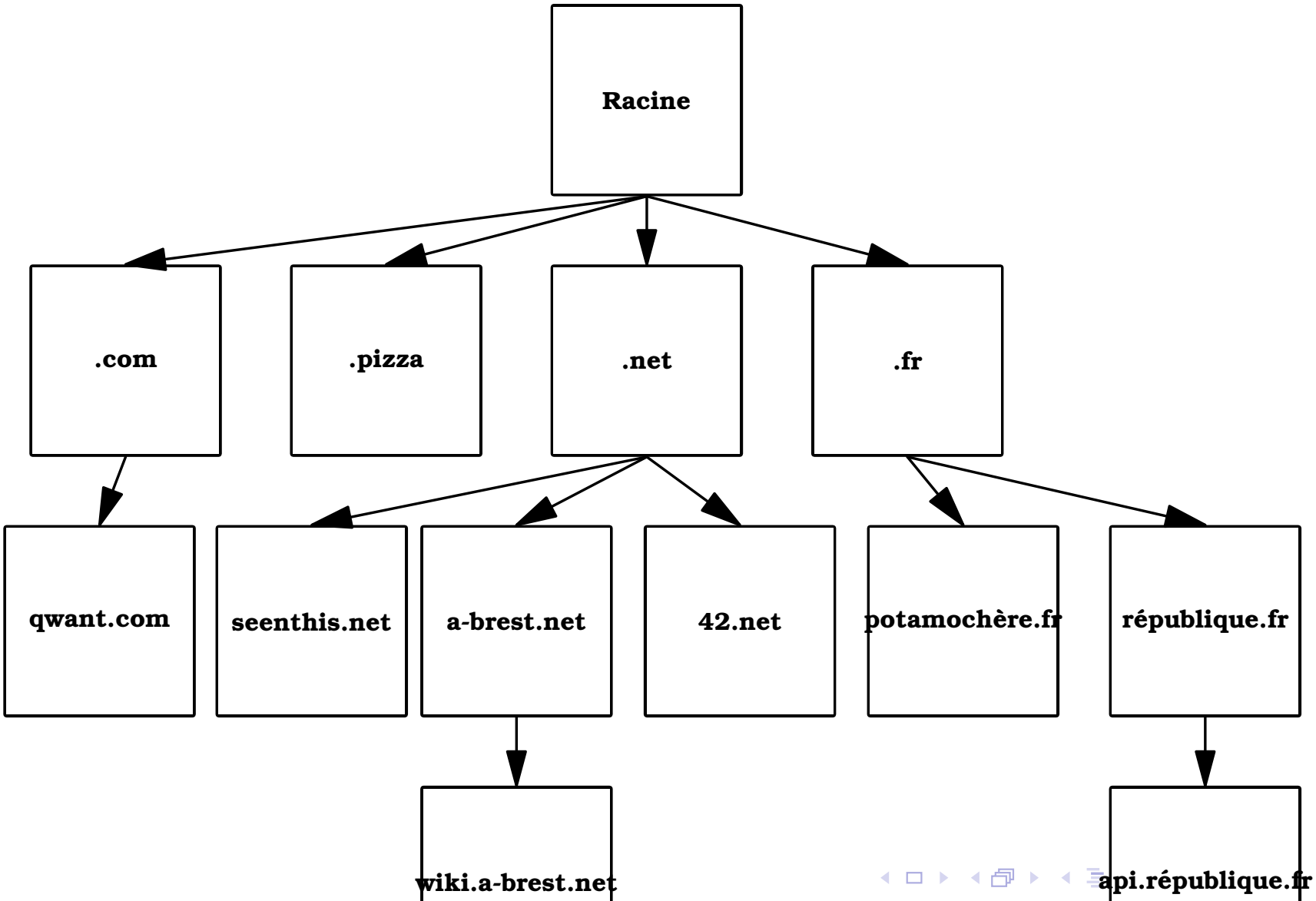
Les noms

- Exemples de noms de domaines : `wiki.a-brest.net`, `www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`, `www.st-cyr.terre.defense.gouv.fr`, `re`, `_sipfederationtls._tcp.en-marche.fr`, `fr.wikipedia.org`, `mamot.fr`...

Les noms

- Exemples de noms de domaines : `wiki.a-brest.net`, `www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`, `www.st-cyr.terre.defense.gouv.fr`, `re`, `_sipfederationtls._tcp.en-marche.fr`, `fr.wikipedia.org`, `mamot.fr`...
- `nca.x.gsi.gov.uk` a cinq composants. Le nom le plus général, le **TLD** (*Top-Level Domain* ou domaine de tête, ici `uk`) est à la fin.

Les noms en arbre



Délégation

Des noms peuvent être **délégués** et on change alors d'organisme responsable. Par exemple `uk.com` est délégué depuis `com` et délègue à son tour.

Rien dans le nom n'indique où est la frontière de délégation : il faut utiliser le DNS.

Le DNS

Les noms sont les identificateurs, le DNS le protocole pour les utiliser.

- Un système de **rendez-vous** avec des noms **stables**

Le DNS

Les noms sont les identificateurs, le DNS le protocole pour les utiliser.

- Un système de **rendez-vous** avec des noms **stables**
- Fait correspondre des noms de domaine à des valeurs (p. ex. adresse IP)

Le DNS

Les noms sont les identificateurs, le DNS le protocole pour les utiliser.

- Un système de **rendez-vous** avec des noms **stables**
- Fait correspondre des noms de domaine à des valeurs
- Indispensable à quasiment toutes les transactions Internet

Le DNS

Les noms sont les identificateurs, le DNS le protocole pour les utiliser.

- Un système de **rendez-vous** avec des noms **stables**
- Fait correspondre des noms de domaine à des valeurs
- Indispensable à quasiment toutes les transactions Internet
- Infrastructure donc invisible, donc difficile d'avoir un budget

Plan du tutoriel

C'est quoi, la sécurité ?

Nous voulons tous de la **sécurité** pour nos noms.

Mais quel genre de sécurité ?

1. Contre les pannes ?
    1. Physiques ?
    2. Logicielles ?
2. Contre les attaques ? Menées par qui ?
    1. L'État ?
    2. Le lycéen dans son garage ?
    3. La mafia ?
3. Contre les cafouillages administratifs ?
    1. Non-renouvellement
    2. Détournement

SécuritéS

Il n'y a pas **la** sécurité. Il y a **plusieurs** services de sécurité, parfois contradictoires :

1. La disponibilité (le service fonctionne)
2. L'intégrité (le service n'a pas été modifié subrepticement)
3. La confidentialité (le service ne laisse pas fuire des informations)

Disponibilité et intégrité s'entendent souvent mal.

Observations des problèmes

On voit rarement des observations sérieuses des incidents (exemple, la panne de “.au” du 13 février 2017.) On ne teste pas le DNS avec un navigateur Web ! On utilise ces outils :

1. dig, client DNS très largement disponible

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare (mais qui teste tous les serveurs d'une zone)

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/` (tests détaillés de la zone)

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/`
4. DNSviz `https://dnsviz.net/` (idem, surtout DNSSEC et visualisation graphique)

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/`
4. DNSviz `https://dnsviz.net/`
5. Sondes RIPE Atlas. Contrairement aux outils précédents, marchent depuis plusieurs points (le résultat dépend du point de mesure).

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/`
4. DNSviz `https://dnsviz.net/`
5. Sondes RIPE Atlas. Contrairement aux outils précédents, marchent depuis plusieurs points.
   - Petit boitier matériel que des volontaires installent,

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/`
4. DNSviz `https://dnsviz.net/`
5. Sondes RIPE Atlas. Contrairement aux outils précédents, marchent depuis plusieurs points.
   - Petit boitier matériel que des volontaires installent,
   - Effectue des mesures actives,

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/`
4. DNSviz `https://dnsviz.net/`
5. Sondes RIPE Atlas. Contrairement aux outils précédents, marchent depuis plusieurs points.
   - Petit boitier matériel que des volontaires installent,
   - Effectue des mesures actives,
   - Qui peuvent être décidées par les utilisateurs.

Observations des problèmes

On voit rarement des observations sérieuses des incidents On utilise ces outils :

1. dig, client DNS très largement disponible
2. check_soa, client DNS plus rare
3. Zonemaster `https://zonemaster.net/`
4. DNSviz `https://dnsviz.net/`
5. Sondes RIPE Atlas. Contrairement aux outils précédents, marchent depuis plusieurs points.
   - Petit boitier matériel que des volontaires installent,
   - Effectue des mesures actives,
   - Qui peuvent être décidées par les utilisateurs.
6. Bases « *Passive DNS* » qui récoltent les réponses DNS auprès de résolveurs et les stockent (permet le voyage dans le temps)

Plan du tutoriel

La résolution DNS

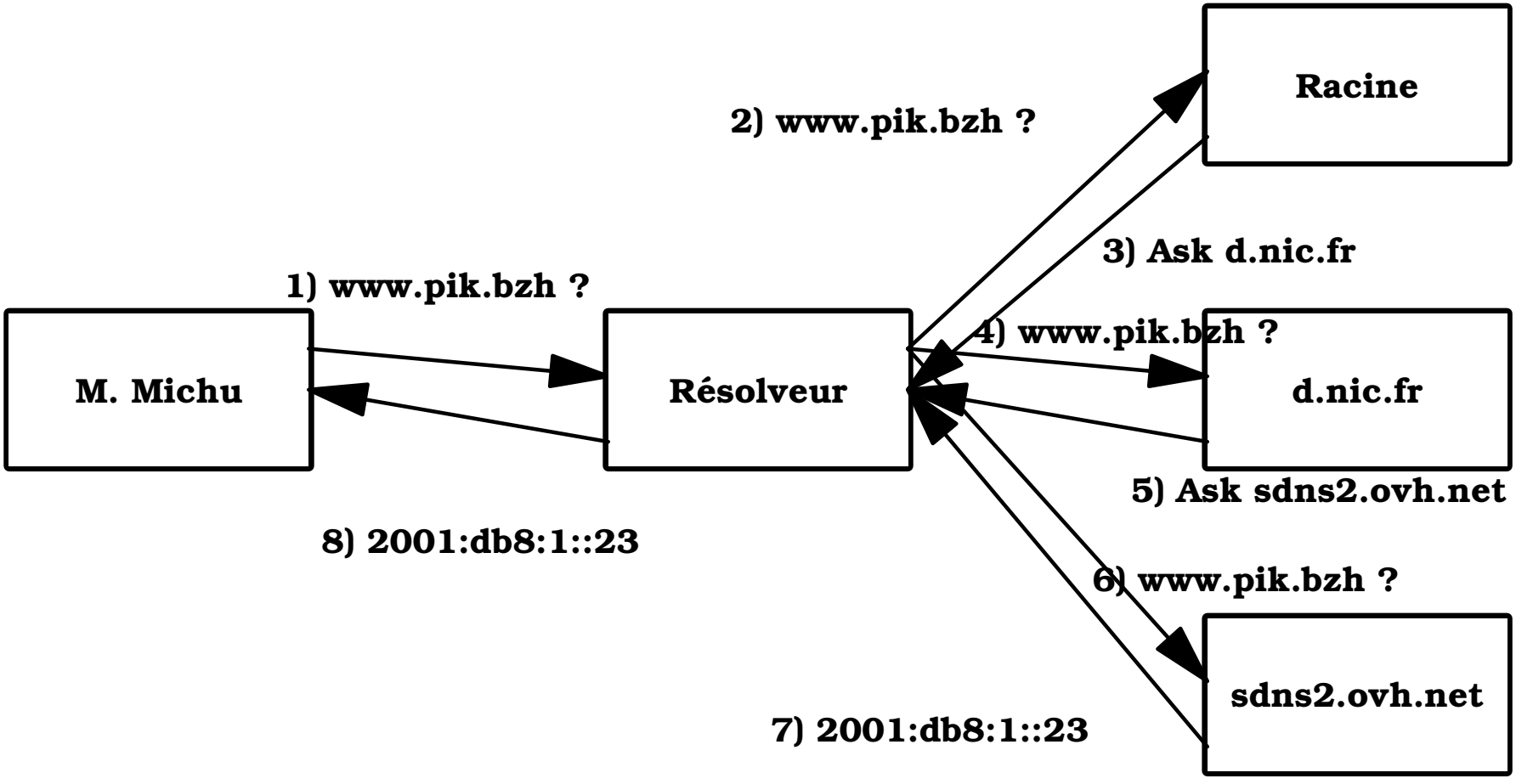
Résolution : demander aux serveurs DNS les informations associées à un nom de domaine (par exemple les adresses IP)

Il y a les serveurs **résolveurs** (typiquement fournis par le FAI) et les serveurs **faisant autorité** (ceux des titulaires de noms ou d'un hébergeur DNS).

Vocabulaire important

- **Résolveur** (ou serveur récursif) : serveur DNS qui ne connait rien mais pose des questions aux serveurs faisant autorité et mémorise les réponses. Chez le FAI, ou sur le réseau local ou encore chez Google ou Cloudflare.
- **Serveur faisant autorité** : serveur DNS qui connait le contenu d'un domaine. Exemple : les serveurs de l'AFNIC qui connaissent ce qu'il y a dans `.fr` et peuvent répondre. Ou les serveurs de `lacantine.org` (chez Bearstech)

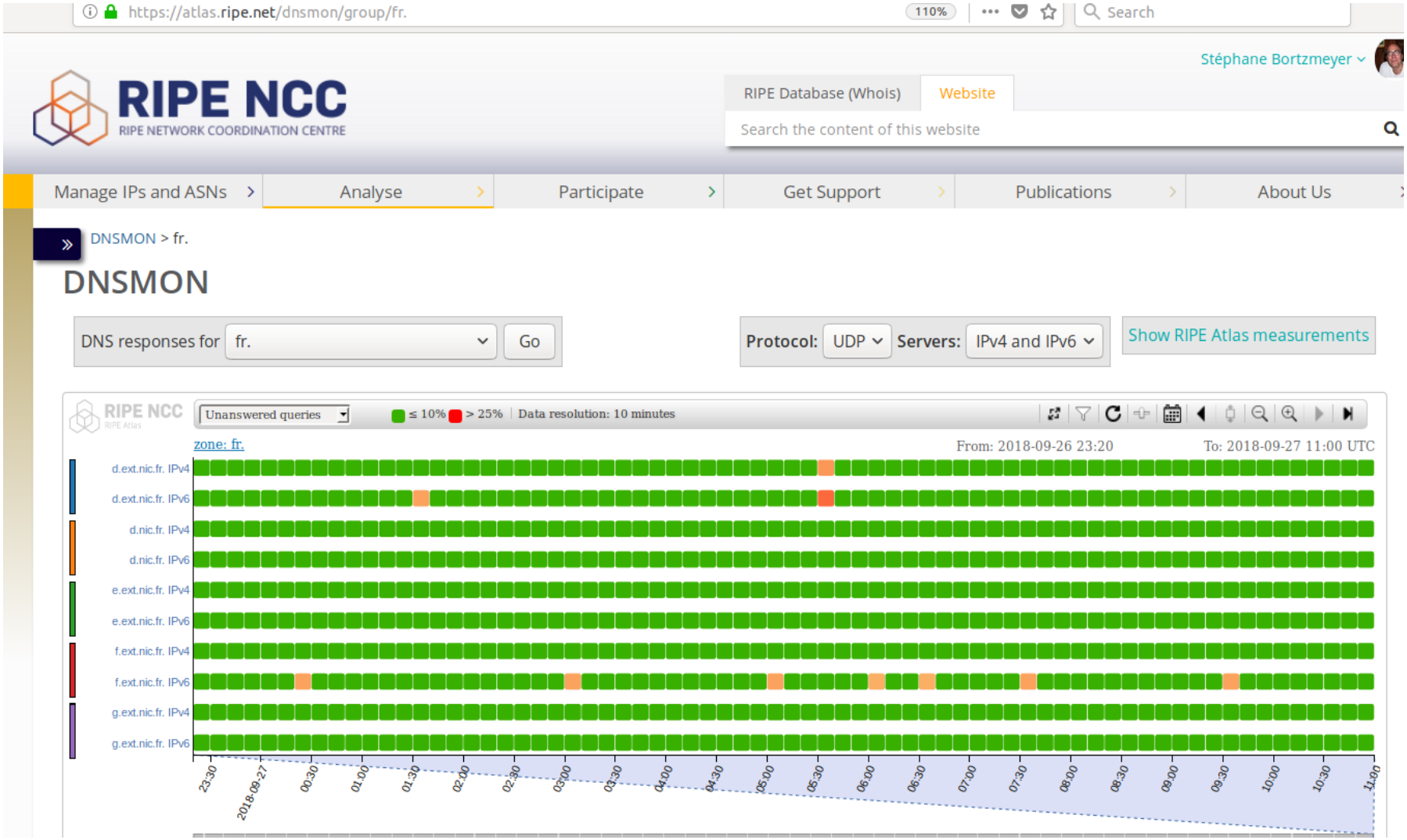
La résolution DNS



Avec le client DNS dig

```
% dig AAAA www.bortzmeyer.org
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10633
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
www.bortzmeyer.org. 7013 IN AAAA 2001:4b98:dc0:41:216:3eff:fe27:3d3f
www.bortzmeyer.org. 7013 IN AAAA 2605:4500:2:245b::42
...
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Sep 27 13:06:44 CEST 2018
;; MSG SIZE  rcvd: 103
```

Exemple de surveillance continue

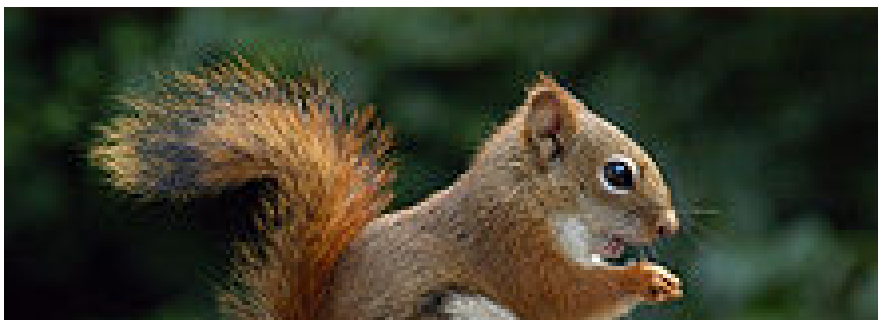


https://atlas.ripe.net/dnsmon/

Pannes matérielles

Plein d'ennemis possibles :

- Pelleteuses (coupure de Prosodie en mai 2011)
- Personne du ménage
- Bâteau de pêche (dont l'ancre arrache les câbles)
- Écureuil (aux États-Unis, les câbles ne sont pas enterrés)



Problème de routage et/ou du serveur résolveur

Problème de routage et/ou du serveur résolveur

- Orange se trompe dans la configuration de la censure et redirige Google et Wikipédia vers le Ministère de l'Intérieur (octobre 2016)

Problème de routage et/ou du serveur résolveur

- Orange se trompe dans la configuration de la censure et redirige Google et Wikipédia vers le Ministère de l'Intérieur (octobre 2016)
- Problème de routage partiel chez Orange, les résolveurs perdent une partie de leur connectivité (novembre 2016)

Problème de routage et/ou du serveur résolveur

- Orange se trompe dans la configuration de la censure et redirige Google et Wikipédia vers le Ministère de l'Intérieur (octobre 2016)
- Problème de routage partiel chez Orange, les résolveurs perdent une partie de leur connectivité (novembre 2016)
- Plusieurs pannes totales des résolveurs Free en janvier 2017

Un domaine peu résilient

```
% check-soa -i minmujer.gob.ve
dns1.minmujer.gob.ve.
        200.109.64.94: OK: 2015020401 (203 ms)
dns2.minmujer.gob.ve.
        200.109.64.93: ERROR: read udp 200.109.64.93:53: i/o timeout
```

Autre exemple, la panne DNS de “impots.gouv.fr” en Avril 2016 (serveurs accessibles depuis certains réseaux seulement)

```
% blaeu-resolve --requested 500 --country FR --type A impots.gouv.fr
[ERROR: SERVFAIL] : 177 occurrences
[145.242.11.48] : 213 occurrences
[TIMEOUT(S)] : 107 occurrences
Test #3645793 done at 2016-04-05T10:01:16Z
```

Autre domaine peu résilient

Tous les serveurs faisant autorité du TLD `.pf` en panne DNS (ping marchait) en avril 2018. Les caches ont un peu aidé

```
% blaeu-resolve --requested 100 --type NS vini.pf
[TIMEOUT(S)] : 41 occurrences
[ERROR: SERVFAIL] : 48 occurrences
[ns1.mana.pf. ns2.mana.pf.] : 5 occurrences
Test #12237080 done at 2018-04-20T06:46:50Z
```

Idem pour `finances.gouv.fr` en mars 2018.

Pannes logicielles

La seconde qui tue

Le 1er juillet 2012, une bogue Linux liée à la seconde intercalaire plante de nombreux serveurs. Dont tous ceux du NIST (bureau états-unien des mesures). Tous les serveurs de `time.gov` sont en panne.

La seconde qui tue, suite

Pareil pour les DNS faisant autorité chez CloudFlare le 1er janvier 2017

Attaque par déni de service

Déni de service : attaque qui vise à empêcher le service de fonctionner.

Il ne s'agit pas de prendre le contrôle du service, juste de l'arrêter. Par exemple, envoi d'une énorme quantité de données au serveur. . . qui n'arrive plus à suivre. Il ne peut plus alors répondre aux requêtes légitimes. Se défendre contre ces attaques est **très** difficile.

Exemples d'attaques par déni de service

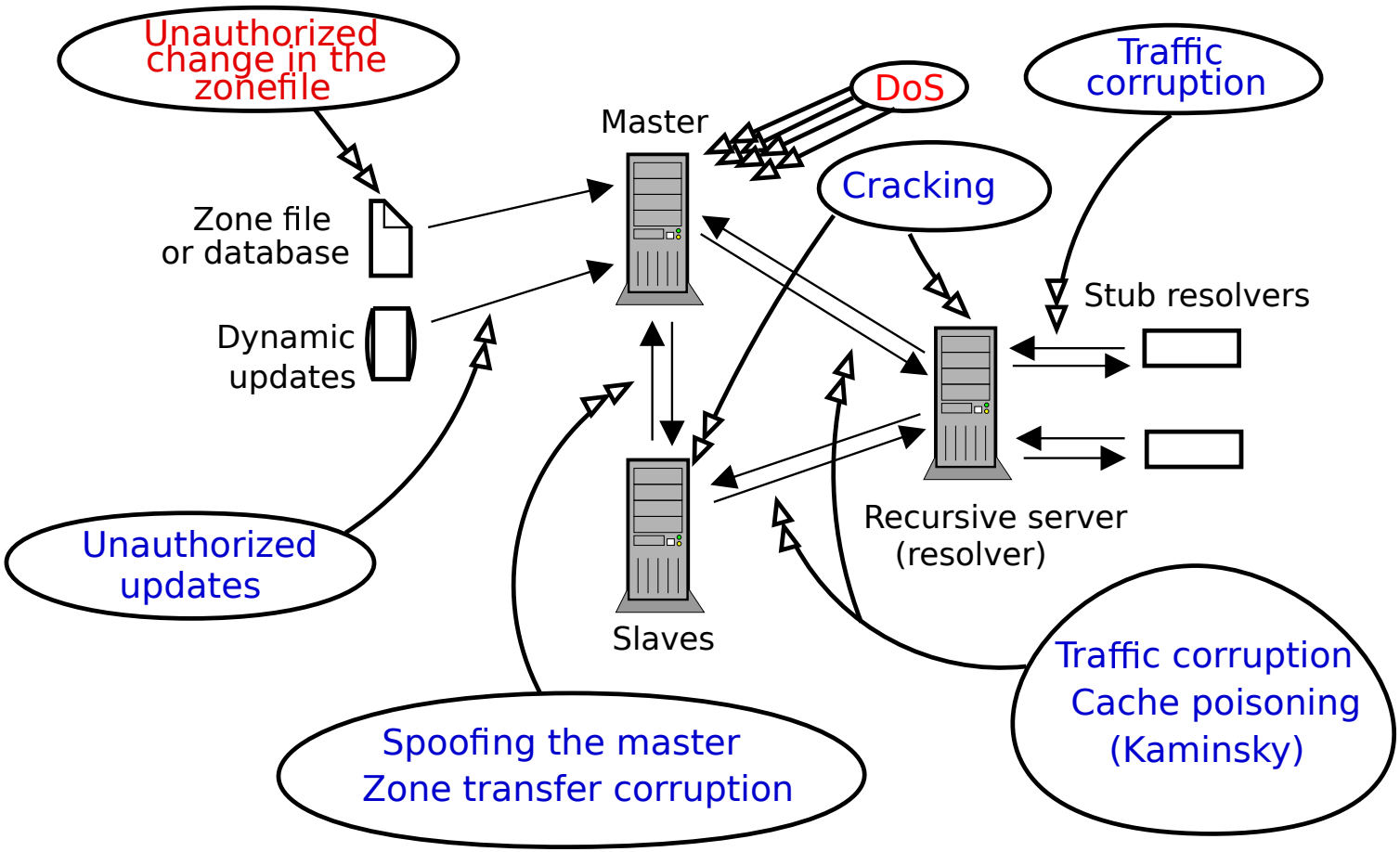
- Novembre/Décembre 2015, puis Juin 2016, attaque contre les serveurs racine. Pas mal de timeouts sur certains serveurs, aucune conséquences visible pour l'utilisateur.
- TLD "`.tr`" complètement arrêté en Décembre 2015
- Octobre 2016, attaque contre Dyn, gros hébergeur DNS. Service quasiment interrompu, plusieurs domaines ne marchent plus (en plantant d'autres à leur tour).

Attaque contre KickAss, janvier 2016

```
% check-soa -i kat.cr
ns1.kat.cr.
    93.190.142.169: OK: 1452860838 (27 ms)
ns2.kat.cr.
    62.210.152.197: OK: 1452860838 (5 ms)
ns3.kat.cr.
    193.24.208.252: ERROR: read udp 193.24.208.252:53: i/o timeout
ns4.kat.cr.
    195.3.147.99: ERROR: read udp 195.3.147.99:53: i/o timeout
ns5.kat.cr.
    94.199.48.231: ERROR: read udp 94.199.48.231:53: i/o timeout
```

Attaque contre la racine de juin 2016, vue par DNSmon

Menaces DNS


Unauthorized change in the zonefile
DoS
Traffic corruption
Master
Cracking
Zone file or database
Dynamic updates
Stub resolvers
Unauthorized updates
Recursive server (resolver)
Slaves
Traffic corruption
Cache poisoning
(Kaminsky)
Spoofing the master
Zone transfer corruption

Modification des requêtes ou réponses dans le réseau

Problème surtout étudié en Chine

À l'intérieur du réseau, les réponses DNS sont modifiées (même si on avait demandé directement à un serveur étranger).

Modification des requêtes ou réponse par le résolveur

Résolveurs menteurs

Résolveurs du FAI qui donnent délibérement de fausses réponses. Motivation la plus courante : rediriger vers des pages de pub.

Censure légale

ARJEL, tribunaux, Ministère de l'Intérieur en France, équivalents dans plein d'autres pays : le résolveur DNS a l'obligation légale de mentir (« `www.romecasino.com` n'existe pas »)

Exemple de censure en France, vu par les sondes Atlas

```
% blaeu-resolve --country FR  --requested 500 --type A thepiratebay.se
Measurement #2420872 for thepiratebay.se/A uses 500 probes
[141.101.118.194 141.101.118.195] : 239 occurrences
[ERROR: NXDOMAIN] : 21 occurrences
[146.112.61.106] : 2 occurrences
[ERROR: SERVFAIL] : 31 occurrences
[127.0.0.1] : 184 occurrences
Test done at 2015-09-16T07:43:43Z
```

Empoisonnement de cache (Kaminsky)

- Un pirate peut répondre au résolveur, **avant** le serveur légitime,
- DNS tourne sur UDP qui ne protège pas contre l'usurpation d'adresse
- Découverte en janvier 2008 par Dan Kaminsky, annoncée le 8 juillet 2008 puis publiée en août.
- A nécessité de *patcher* la plupart des **résolveurs** pour mettre des ports sources aléatoires (RFC 5452).
- Exploite uniquement des failles connues mais avec un moyen de les rendre mille fois plus efficace. L'empoisonnement DNS était théoriquement possible, il devient facile.

Changement de résolveur

1. Les machines font une confiance aveugle à leur résolveur (peu valident elles-même avec DNSSEC).
2. Changer le résolveur permet de tout faire (le résolveur du méchant peut alors répondre que `www.mabanque.example` est `192.0.2.1`, adresse contrôlée par le méchant).

Exemple :DNS Changer

Logiciel malveillant qui changeait les résolveurs. Le trafic était détourné vers des sites Web payants. Le FBI a piraté les résolveurs du méchant pour analyser le trafic.

Surveillance

Le trafic DNS nous en apprend beaucoup. . .

Tout gérant de serveur (faisant autorité ou résolveur) peut en apprendre sur les utilisateurs. Par défaut, les requêtes DNS circulent en clair, et elles sont très détaillées (RFC 7626 pour l'analyse des risques). « Vous avez consulté `www.djihad.sa`, `pornhub.com` et `alcooliques-anonymes.fr`. »

Attaques non techniques

- La lecture de certains journaux pourrait le faire oublier mais les attaques les plus courantes sont non techniques.
- Ingéniérie sociale (« j'ai oublié le nom du fichier où il y avait le mot de passe, vous pouvez me le rappeler ? »)
- Un bon exemple est le hameçonnage « votre compte vient d'être crédité de 10 000 $, allez en `http://192.0.2.1/form.php` pour valider ce transfert »

Plan du tutoriel

Enregistrement des noms

Les noms de domaine sont enregistrés auprès d'un **registre**, souvent via un **Bureau d'Enregistrement (BE)**, et hébergés chez un **hébergeur DNS** (souvent le BE).

Chacun de ces acteurs peut être défaillant

Par piratage ou malhonnêteté

Piratage chez l'utilisateur

Piratage chez l'utilisateur

- Canal+ en mars 2016

Piratage chez l'utilisateur

- Canal+ en mars 2016
- Météo France en mai 2016

Piratage chez l'utilisateur

- Canal+ en mars 2016
- Météo France en mai 2016
- "`blockchain.info`" détourné en octobre 2016 (pour piquer des bitcoins)

Analyse d'un détournement, a posteriori, avec DNSDB

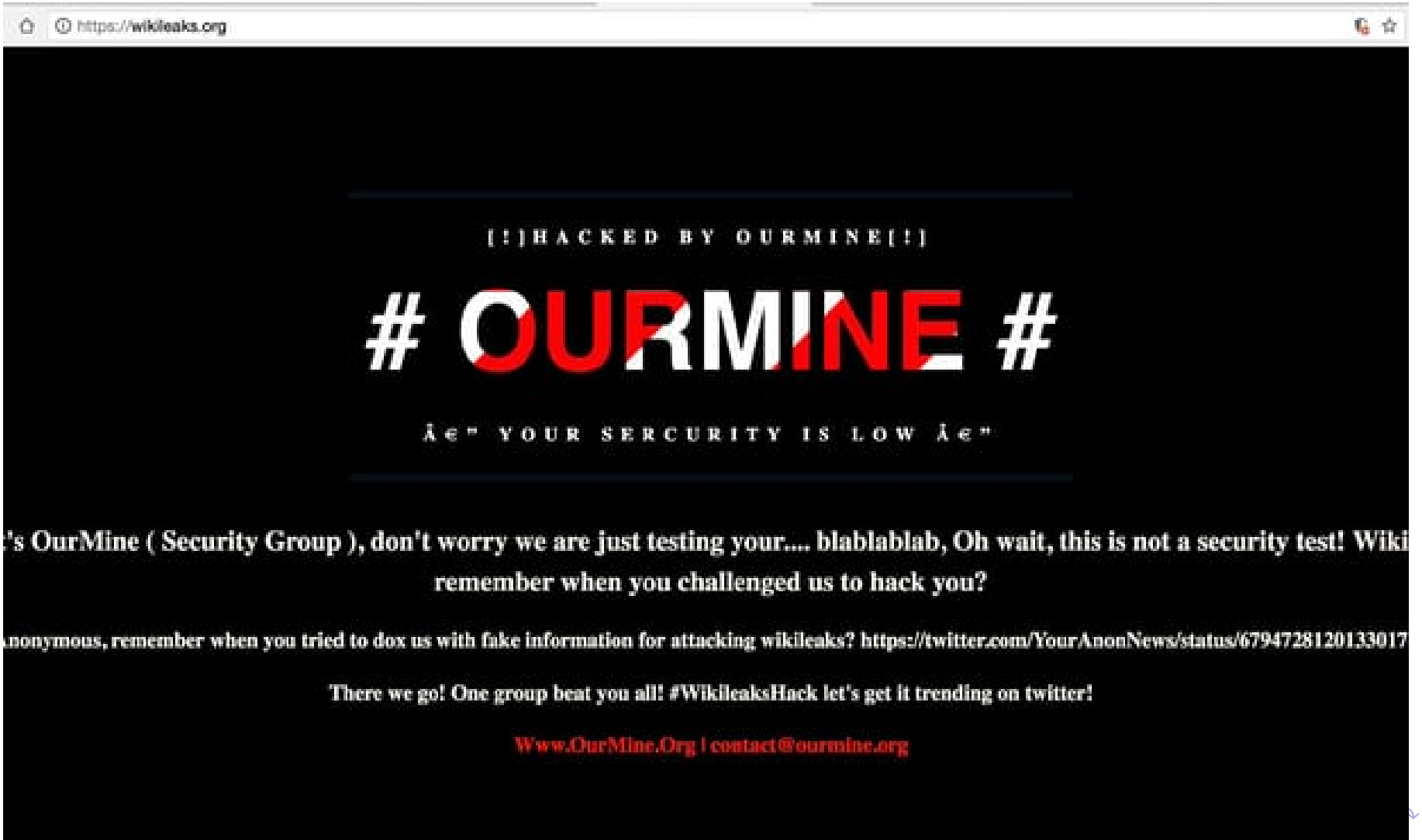
```
NORMALEMENT
;; bailiwick: fr.
;;
count: 116142
;; first seen: 2012-11-26 10:28:11 -0000
;; last seen: 2016-09-01 13:04:31 -0000
meteofrance.fr. IN NS vivaldi.meteo.fr.
meteofrance.fr. IN NS cadillac.meteo.fr.

PENDANT LE DÉTOURNEMENT
;; bailiwick: fr.
;;
count: 57
;; first seen: 2016-05-23 22:33:49 -0000
;; last seen: 2016-05-24 08:00:57 -0000
meteofrance.fr. IN NS ns1.hostinger.fr.
meteofrance.fr. IN NS ns2.hostinger.fr.
meteofrance.fr. IN NS ns3.hostinger.fr.
meteofrance.fr. IN NS ns4.hostinger.fr.
```

Que s'est-il passé le 30 août 2017 ?

Que s'est-il passé le 30 août 2017 ?

Le visiteur de `https://wikileaks.org/` voyait :



Les faits

Utilisation d'une base de « *passive DNS* », DNSDB :

```
;;  bailiwick: org.
;; first seen: 2017-08-30 04:20:15 -0000
;;  last seen: 2017-08-30 04:28:41 -0000
wikileaks.org. IN NS ns1.rival-dns.com.
wikileaks.org. IN NS ns2.rival-dns.com.
wikileaks.org. IN NS ns3.rival-dns.com.

;;  bailiwick: org.
;; first seen: 2017-08-30 04:28:40 -0000
;;  last seen: 2017-08-30 04:30:28 -0000
wikileaks.org. IN NS ns1.rivalhost.com.
wikileaks.org. IN NS ns2.rivalhost.com.
wikileaks.org. IN NS ns3.rivalhost.com.

;;  bailiwick: wikileaks.org.
;; first seen: 2017-08-31 02:02:38 -0000
;;  last seen: 2017-08-31 02:02:38 -0000
```

Interprétation

Interprétation

- Le serveur Web n'a pas été touché,

Interprétation

- Le serveur Web n'a pas été touché,
- L'attaque a bien eu lieu et a été un succès,

Interprétation

- Le serveur Web n'a pas été touché,
- L'attaque a bien eu lieu et a été un succès,
- Après, tout est une question de vocabulaire. . .

Interprétation

- Le serveur Web n'a pas été touché,
- L'attaque a bien eu lieu et a été un succès,
- Après, tout est une question de vocabulaire. . .
- Et de modèle de menace (attaque contre l'image, ou bien contre les données sur le serveur).

Que s'est-il passé pour Wikileaks ?

Que s'est-il passé pour Wikileaks ?

- On ne sait pas,

Que s'est-il passé pour Wikileaks ?

- On ne sait pas,
- Wikileaks n'a rien publié,

Que s'est-il passé pour Wikileaks ?

- On ne sait pas,
- Wikileaks n'a rien publié,
- Même s'ils l'avaient fait, on ne saurait pas si c'est vrai,

Que s'est-il passé pour Wikileaks ?

- On ne sait pas,
- Wikileaks n'a rien publié,
- Même s'ils l'avaient fait, on ne saurait pas si c'est vrai,
- Disons juste que les faits observés sont compatibles avec l'hypothèse d'un piratage du compte Wikileaks au BE/hébergeur.

Piratage d'un BE

Notez qu'il n'est pas toujours facile de savoir si c'est le BE ou le titulaire qui a été piraté...

Piratage d'un BE

Notez qu'il n'est pas toujours facile de savoir si c'est le BE ou le titulaire qui a été piraté...

- Cas de "`google.co.ma`" en 2009 Piratage du BE (injection SQL) puis envoi des fausses données au registre

Piratage d'un BE

Notez qu'il n'est pas toujours facile de savoir si c'est le BE ou le titulaire qui a été piraté...

- Cas de "`google.co.ma`" en 2009
- Ou bien la SEA (Syrian Electronic Army) en Août 2013 (`nytimes.com` détourné)

Piratage d'un BE

Notez qu'il n'est pas toujours facile de savoir si c'est le BE ou le titulaire qui a été piraté...

- Cas de "`google.co.ma`" en 2009
- Ou bien la SEA (Syrian Electronic Army) en Août 2013 (`nytimes.com` détourné)
- Ou encore "`google.com.br`" en janvier 2017

Cafouillage administratif

Cafouillage administratif

- Renouvellement du nom non payé,

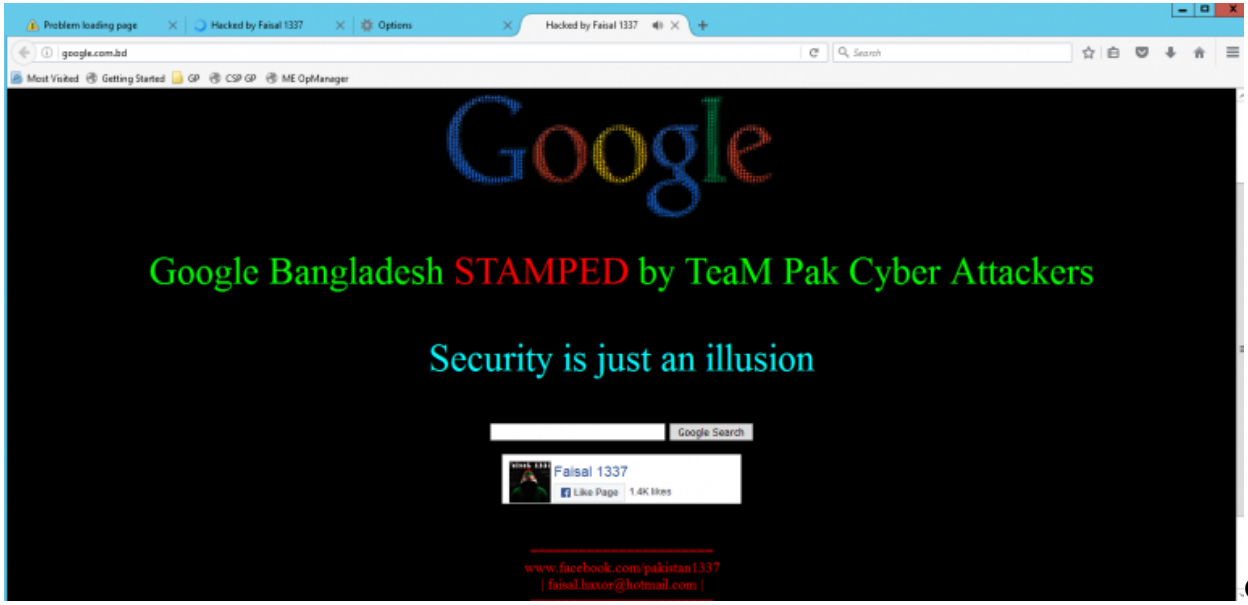
Cafouillage administratif

- Renouvellement du nom non payé,
- Ou conflit entre client et BE,

Cafouillage administratif

- Renouvellement du nom non payé,
- Ou conflit entre client et BE,
- `letsencrypt.org` plus publié dans le DNS en juillet 2018 : le BE l'avait mis *on hold*.

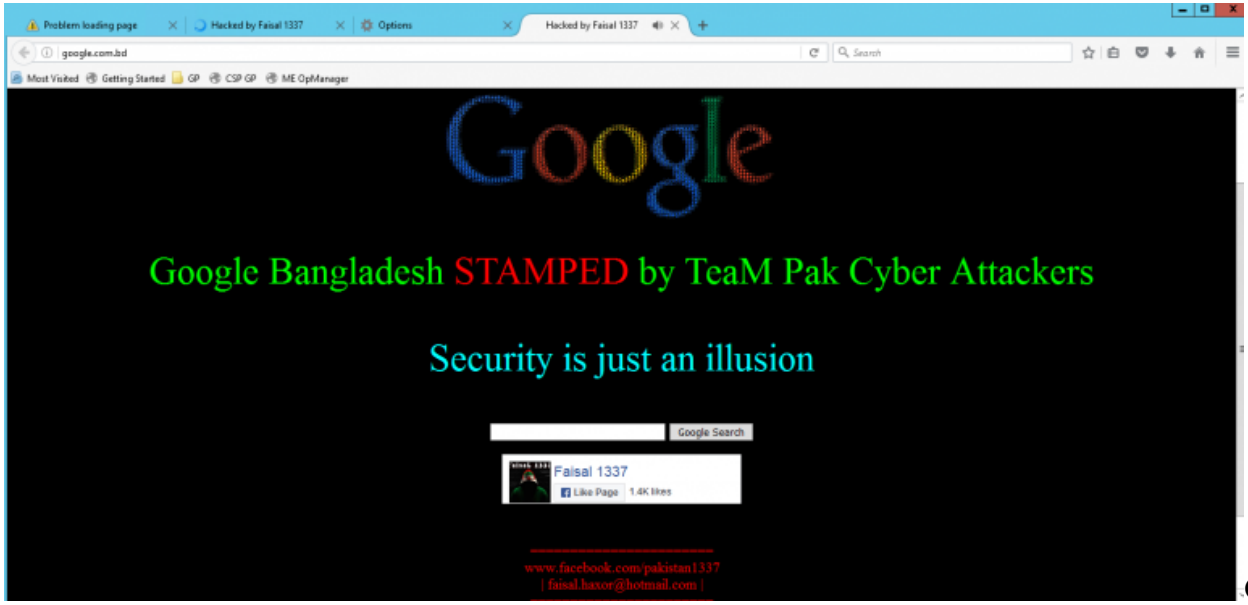
Piratage d'un registre



Copie d'écran prise par Farhad Ahmed

Piratage d'un registre

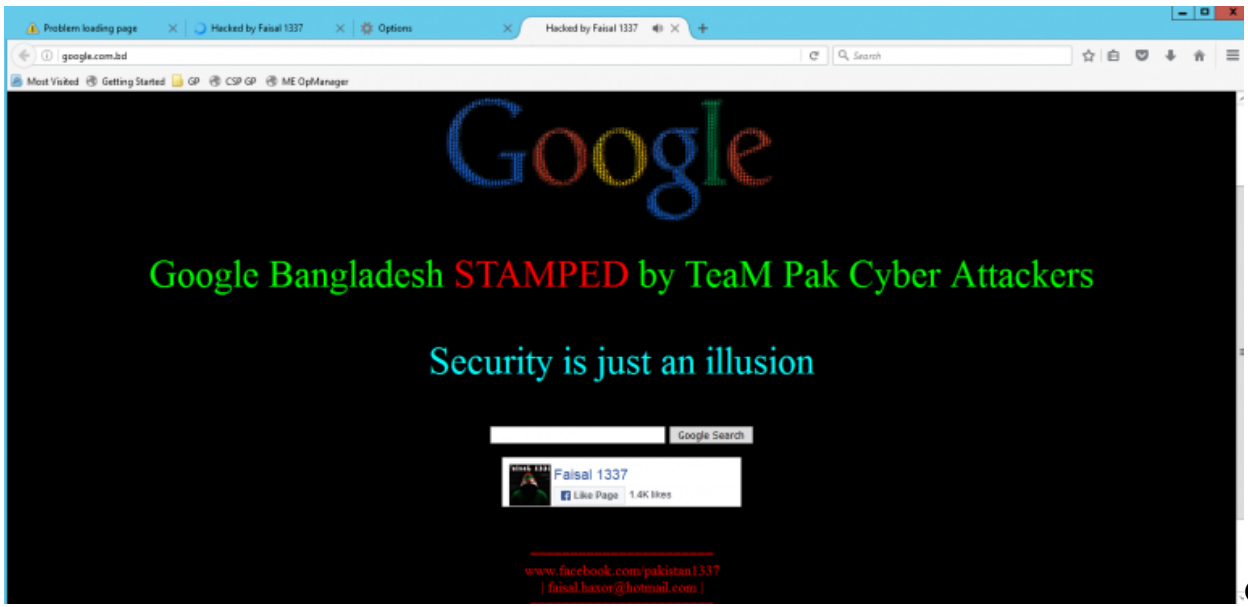
- ".bd" en Décembre 2016



Copie d'écran prise par Farhad Ahmed

Piratage d'un registre

- "`.bd`" en Décembre 2016
- Faille détectée (mais non exploitée) dans "`.as`" en Juin 2016



Copie d'écran prise par Farhad Ahmed

Bien plus sophistiqué, MyEtherWallet

Bien plus sophistiqué, MyEtherWallet

- Avril 2018, détournement BGP pour capter le trafic des serveurs faisant autorité de Route 53 (Amazon),

Bien plus sophistiqué, MyEtherWallet

- Avril 2018, détournement BGP pour capter le trafic des serveurs faisant autorité de Route 53 (Amazon),
- Réponses mensongères pour le domaine `myetherwallet.com` (portefeuilles de cryptomonnaie)

Saisie légale

Opération « *In Our Sites* »

L'ICE (*U.S. Immigration and Customs Enforcement*, agence états-unienne) a saisi auprès du registre de `.com` des centaines de noms (sans jugement).

La loi est nationale

Bien se rappeler qu'il n'existe pas de TLD « international ».

Vous utilisez un `.com`, vous êtes soumis à la loi états-unienne.

Se faire prendre son domaine légalement en France

- Pas de garantie pour le titulaire de noms de domaine
- Le domaine peut être pris au titulaire de bonne foi, par jugement (affaire Milka en 2005) ou bien par menaces juridiques (affaire Madame Figaro en 2012).

Détournement

Manœuvres pour mettre la main sur un domaine (envoi de faux messages du titulaire, par exemple)

Connu grâce au célébrissime `sex.com` qui a ainsi changé de mains plusieurs fois (et qui a fait l'objet d'un livre, le seul nom de domaine dans ce cas)

Plan du tutoriel

Certains risques sont surtout pour les conférences sécurité

1. Les orateurs aux conférences sécurité aiment bien les exposés techniques rigolos, même s'ils sont irréalistes.
2. Dans ces conférences, on voit donc souvent passer des « vulnérabilités » qui ne marcheront qu'en labo.

Exemple, les IDN

1. En outre, dans ces conférences, tout le monde parle anglais : on est donc sûr d'obtenir un succès en attaquant Unicode.
2. Exemple de légende urbaine répandue « Les IDN facilitent le hameçonnage, `cìc.fr` ressemble à `cic.fr` ».
3. Or, toutes les études sur le hameçonnage montrent que les utilisateurs ignorent l'URL, ne le comprenant pas (`cic-secure.com...`).
4. Les spams de hameçonnage ne comprennent pas d'IDN et souvent uniquement des adresses IP !
5. Mais le monde de la sécurité informatique n'est pas encore *evidence-based*. Les légendes ont la vie dure.

Les attaques les plus courantes

Les attaques purement DNS sont très minoritaires

Ne vous focalisez pas sur les attaques techniques sophistiquées qui font la une. La plupart des attaques sont « bêtes » mais efficaces (ingéniérie sociale, faille exploitée par un *script-kiddie*, dDoS purement volumétrique).

Exemple : le rapport Fireeye de janvier 2019 sur les détournements de noms

Plan du tutoriel

Redondance

Redondance

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début (contrairement à HTTP),

Redondance

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début,
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,

Redondance

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début,
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,
3. Sur-avitailler : machines et réseaux pouvant tenir dix à vingt fois la charge normale (pour les cas de dDoS),

Redondance

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début,
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,
3. Sur-avitailler : machines et réseaux pouvant tenir dix à vingt fois la charge normale,
4. Et, surtout, évitez le SPOF (*Single Point of Failure*). Ayez plusieurs sites physiques et, si possible, plusieurs opérateurs... Exemple : "`pornhub.com`" était chez Dyn **et** chez UltraDNS. Pas de panne le 21 octobre 2017.

Redondance

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début,
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,
3. Sur-avitailler : machines et réseaux pouvant tenir dix à vingt fois la charge normale,
4. Et, surtout, évitez le SPOF. Ayez plusieurs sites physiques et, si possible, plusieurs opérateurs. . .
5. Bonne lecture : le Rapport annuel sur le résilience de l'Internet en France (ANSSI/AFNIC).

Diversité

- Une bogue BIND et tous vos domaines sont fichus ?
- Une bogue Linux et, le jour de la seconde intercalaire, aucun serveur ne marche ?

Favoriser la diversité génétique

Par exemple, il n'y a aucune raison de n'utiliser que BIND. « Nous vous rappelons qu'il existe d'autres possibilités. »

Supervision

- Surveiller l'état de ses domaines, pour éviter d'être prévenus par Slashdot et Zataz... (Surveiller le serveur Web est insuffisant.)
- Surveiller chaque serveur (autrement, vous serez prévenus seulement lorsque le dernier tombera en panne.)

Bonnes pratiques de sécurité

Rien de spécifique aux noms de domaines, mais :

Bonnes pratiques de sécurité

Rien de spécifique aux noms de domaines, mais :

1. Bien vérifier la sécurité du système d'enregistrement (ne pas mettre le mot de passe de votre compte auprès du BE sur un post-it sur l'écran), et de l'hébergement DNS,

Bonnes pratiques de sécurité

Rien de spécifique aux noms de domaines, mais :

1. Bien vérifier la sécurité du système d'enregistrement (ne pas mettre le mot de passe de votre compte auprès du BE sur un post-it sur l'écran), et de l'hébergement DNS,
2. Attention à l'ingéniérie sociale (« Bonjour, ici le service technique de votre *registrar*, il y a un problème technique, nous aurions besoin du mot de passe. »)

Bonnes pratiques de sécurité

Rien de spécifique aux noms de domaines, mais :

1. Bien vérifier la sécurité du système d'enregistrement (ne pas mettre le mot de passe de votre compte auprès du BE sur un post-it sur l'écran), et de l'hébergement DNS,
2. Attention à l'ingéniérie sociale (« Bonjour, ici le service technique de votre *registrar*, il y a un problème technique, nous aurions besoin du mot de passe. »)
3. Développer une culture de sécurité informatique dans le service (juridique, comm'...) qui gère les noms de domaines,

Bonnes pratiques de sécurité

Rien de spécifique aux noms de domaines, mais :

1. Bien vérifier la sécurité du système d'enregistrement (ne pas mettre le mot de passe de votre compte auprès du BE sur un post-it sur l'écran), et de l'hébergement DNS,
2. Attention à l'ingéniérie sociale (« Bonjour, ici le service technique de votre *registrar*, il y a un problème technique, nous aurions besoin du mot de passe. »)
3. Développer une culture de sécurité informatique dans le service (juridique, comm'...) qui gère les noms de domaines,
4. Superviser ses noms.

Bonnes pratiques de sécurité

Rien de spécifique aux noms de domaines, mais :

1. Bien vérifier la sécurité du système d'enregistrement (ne pas mettre le mot de passe de votre compte auprès du BE sur un post-it sur l'écran), et de l'hébergement DNS,
2. Attention à l'ingéniérie sociale (« Bonjour, ici le service technique de votre *registrar*, il y a un problème technique, nous aurions besoin du mot de passe. »)
3. Développer une culture de sécurité informatique dans le service (juridique, comm'...) qui gère les noms de domaines,
4. Superviser ses noms.
5. `https://www.ssi.gouv.fr/guide/bonnes-pratiques-pour-lacquisition-et-lexploitation-de-noms-de-domaine/`

3C

- Communication
- Coopération
- Coordination

Trop de gens sont encore isolés dans leur coin, sans utiliser l'information publique, et sans échanger avec les pairs.

DNSSEC

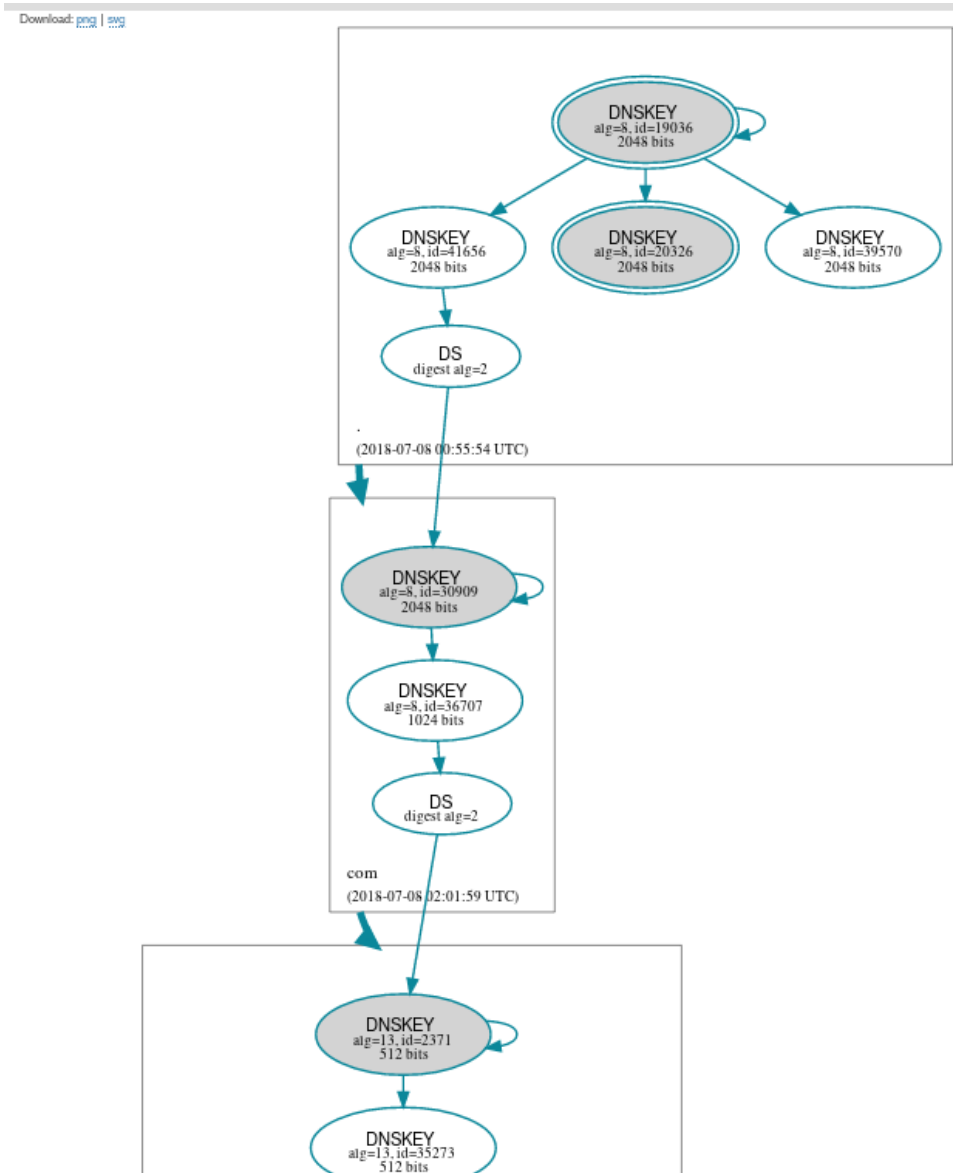
1. Objectif : détecter les empoisonnements de cache
2. Moyen : signature cryptographique des enregistrements

```
% dig A paypal.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17828
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 5, ADDITIONAL: 1
...
;; ANSWER SECTION:
paypal.fr. 300 IN A 64.4.250.13
...
paypal.fr. 300 IN RRSIG A 5 2 300 (
20181013085053 20180913075053 53895 paypal.fr.
VtmpRa4by124vRLsVAjttfgkIJ6OnHCu4UDBp2NrDCSx
...
```

Clés DNSSEC

```
% dig DNSKEY fr
...
;; ANSWER SECTION:
fr. 171353 IN DNSKEY 256 3 8 (
AwEAAbCgB/8XHoSGddV2Kgx+ecaOgOIilTjV8V5KArhT...
) ; ZSK; alg = RSASHA256; key id = 50650
fr. 171353 IN DNSKEY 256 3 8 (
AwEAAbGKnhFuXbQBhpOnQZ7YsiLTQGy73DdbfzUsKUJO...
) ; ZSK; alg = RSASHA256; key id = 24135
fr. 171353 IN DNSKEY 257 3 8 (
AwEAAdR9pshmjn5uOHaEGQaIBBrPK7/nJpGlCxTzhYKo...
) ; KSK; alg = RSASHA256; key id = 42104
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jan 23 17:43:49 UTC 2019
;; MSG SIZE  rcvd: 893
```

DNSSEC, arborescence des clés



DNSSEC, état

1. Tous les TLD importants signés,
2. Mais peu de domaines « utilisateur » signés,
3. Et peu de résolveurs valident (les principaux sont Free en France, Comcast aux USA et Google Public DNS et Cloudflare).

Je veux faire du DNSSEC, mes tâches

1. Signer ses zones.
2. Permettre aux clients de signer les siennes (si on est hébergeur DNS).
3. Activer la validation sur ses résolveurs.

Prévoir

1. Signer des zones nécessite du logiciel sans bogue et une supervision rigoureuse.
2. Activer la validation nécessite de se préparer à la panne d'un domaine important.

Vie privée

Vie privée

- Il faut chiffrer (RFC 7858, DNS-sur-TLS, et RFC 8484, DoH, DNS-sur-HTTPS),

Vie privée

- Il faut chiffrer (RFC 7858, DNS-sur-TLS, et RFC 8484, DoH, DNS-sur-HTTPS),
- Il faut minimiser les données (RFC 7818, à exiger de votre résolveur DNS).

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ? Google ? Cisco ? Cloudflare ?

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ? Google ? Cisco ? Cloudflare ?
- Fiabilité,

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ? Google ? Cisco ? Cloudflare ?
- Fiabilité,
- Performance (**attention**, c'est vraiment difficile à mesurer, notamment cache chaud vs. cache froid),

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ? Google ? Cisco ? Cloudflare ?
- Fiabilité,
- Performance,
- Non-mensonger, ou alors seulement les mensonges que j'approuve,

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ? Google ? Cisco ? Cloudflare ?
- Fiabilité,
- Performance,
- Non-mensonger, ou alors seulement les mensonges que j'approuve,
- Authentifié,

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ? Google ? Cisco ? Cloudflare ?
- Fiabilité,
- Performance,
- Non-mensonger, ou alors seulement les mensonges que j'approuve,
- Authentifié,
- Protégé contre l'écoute, en amont et en aval.

Résolveur du FAI / service informatique

Résolveur du FAI / service informatique

1. Souvent rapide (car proche),

Résolveur du FAI / service informatique

1. Souvent rapide,
2. Fiabilité variable (Orange se trompant et redirigeant vers la Main Rouge le 17 octobre 2016),

Résolveur du FAI / service informatique

1. Souvent rapide,
2. Fiabilité variable,
3. Souvent menteur (Deutsche Telekom ment sur les domaines non existants, les gros FAI français mentent sur ordre de la justice, de l'ARJEL, de la police. . .),

Résolveur du FAI / service informatique

1. Souvent rapide,
2. Fiabilité variable,
3. Souvent menteur,
4. Que font-ils des données ?

Résolveur du FAI / service informatique

1. Souvent rapide,
2. Fiabilité variable,
3. Souvent menteur,
4. Que font-ils des données ?
5. Écoute difficile en amont (mais, en aval, aucun ne fait de *QNAME minimisation*).

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

1. Parfois lointain, donc lent,

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

1. Parfois lointain, donc lent,
2. Fiabilité variable (être joignable 24x7 est difficile),

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

1. Parfois lointain, donc lent,
2. Fiabilité variable,
3. Parfois menteur (Cisco OpenDNS, Quad9),

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

1. Parfois lointain, donc lent,
2. Fiabilité variable,
3. Parfois menteur,
4. Que font-ils des données ? Le RGPD protège-t-il bien, pour des acteurs étrangers ?,

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

1. Parfois lointain, donc lent,
2. Fiabilité variable,
3. Parfois menteur,
4. Que font-ils des données ?,
5. Pas toujours chiffré donc pas authentifié, et vulnérable à l'écoute en amont. En aval, on est « protégé » par le nombre de requêtes.

Son propre résolveur

Peut être sur un PC ou sur une « *box* » qu'on contrôle (brique Internet ?).

Son propre résolveur

Peut être sur un PC ou sur une « *box* » qu'on contrôle.

1. Proche, donc rapide, lorsque le cache est chaud,

Son propre résolveur

Peut être sur un PC ou sur une « *box* » qu'on contrôle.

1. Proche, donc rapide, lorsque le cache est chaud,
2. Aussi fiable que le reste du réseau local,

Son propre résolveur

Peut être sur un PC ou sur une « *box* » qu'on contrôle.

1. Proche, donc rapide, lorsque le cache est chaud,
2. Aussi fiable que le reste du réseau local,
3. Menteur uniquement si on le veut (`googleanalytics.com`),

Son propre résolveur

Peut être sur un PC ou sur une « *box* » qu'on contrôle.

1. Proche, donc rapide, lorsque le cache est chaud,
2. Aussi fiable que le reste du réseau local,
3. Menteur uniquement si on le veut (`googleanalytics.com`),
4. Aucune capture des données (si logiciel libre),

Son propre résolveur

Peut être sur un PC ou sur une « *box* » qu'on contrôle.

1. Proche, donc rapide, lorsque le cache est chaud,
2. Aussi fiable que le reste du réseau local,
3. Menteur uniquement si on le veut (`googleanalytics.com`),
4. Aucune capture des données (si logiciel libre),
5. Vie privée : bonne protection des requêtes amont mais très mauvais pour les requêtes aval (pensez à la *QNAME minimisation*).

Plan du tutoriel

Que faire ?

1. Encore beaucoup de progrès à faire
2. La plupart sur des pratiques de sécurité classiques
3. Quelques nouvelles techniques (DNSSEC, minimisation de la question. . .)