

# DNS, quand il y a encore des problèmes (1/34)

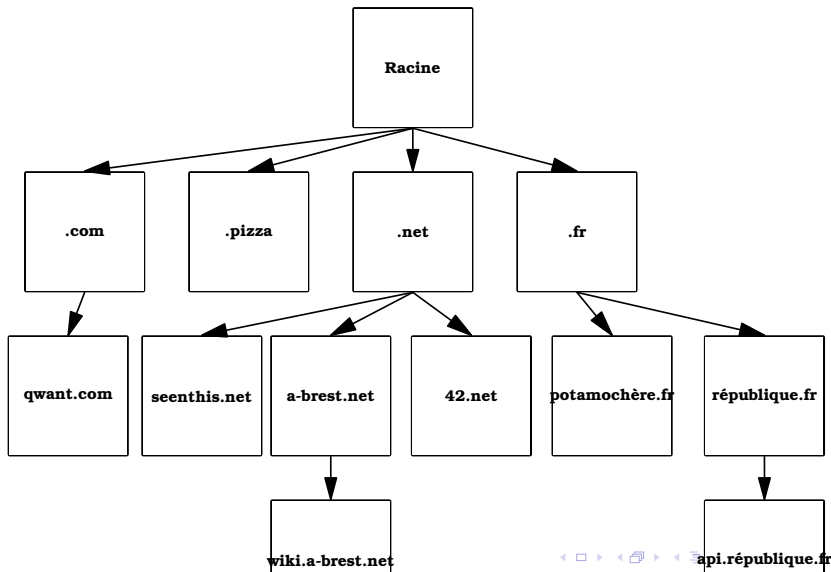
Stéphane Bortzmeyer  
stephane+42@bortzmeyer.org

28 octobre 2019

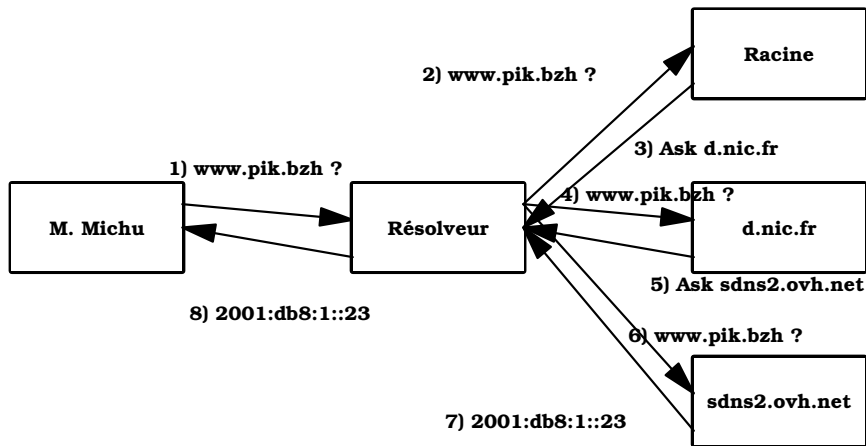
# Plan du tutoriel

- 1 Rappels rapides
- 2 DNSSEC
- 3 Piratage côté avaraillement
- 4 Déni de service
- 5 Vie privée
- 6 Conclusion

# Les noms en arbre



# La résolution DNS



## Avitaillement 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

# Plan du tutoriel

- 1 Rappels rapides
- 2 DNSSEC**
- 3 Piratage côté avaraillement
- 4 Déni de service
- 5 Vie privée
- 6 Conclusion

# DNSSEC

- 1 Objectif : détecter les empoisonnements de cache et les secondaires malveillants ou piratés
- 2 Moyen : signature cryptographique des enregistrements

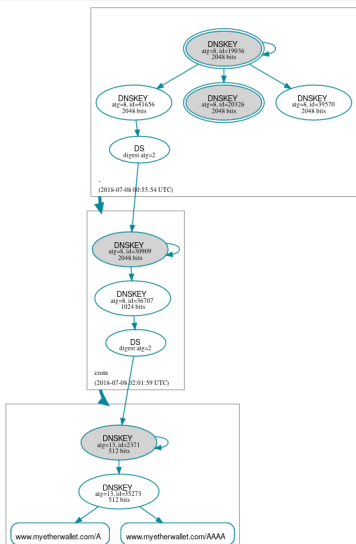
```
% dig A paypal.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17828
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 5, ADDITIONAL: 1
...
;; ANSWER SECTION:
paypal.fr. 300 IN A 64.4.250.13
...
paypal.fr. 300 IN RRSIG A 5 2 300 (
20181013085053 20180913075053 53895 paypal.fr.
VtmpRa4by124vRLsVAjttfgkIJ6OnHCu4UDBp2NrDCSx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

# Clés DNSSEC

```
% dig DNSKEY fr
...
;; ANSWER SECTION:
fr. 171353 IN DNSKEY 256 3 8 (
AwEAAbCgB/8XHoSgddV2Kgx+ecaOg0IilTjV8V5KArhT...
) ; 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 (
AwEAAAdr9pshmjn5uOHaEGQaIBBrPK7/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

Download [png](#) | [svg](#)

# 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. (Exemple des signatures expirées chez ARIN en janvier 2019.)
- 2 Activer la validation nécessite de se préparer à la panne d'un domaine important.

# Plan du tutoriel

- 1 Rappels rapides
- 2 DNSSEC
- 3 Piratage côté avitaillement**
- 4 Déni de service
- 5 Vie privée
- 6 Conclusion

Février 2019...

<https://www.estrepublicain.fr/faits-divers/2019/02/23/gigantesque-cyberattaque-inedite-en-cours-contre-l-infrastr>



Nous suivre

S'identifier

S'ABONNER

☰ NANCY VILLE | NANCY AGGLOMÉRATION | PONT-À-MOUSSON | LUNÉVILLE | TOUL | BAR-LE-DUC | VERDUN | BESANÇON | HAUT-DOUBS | VESOUL-HAUTE SAÔNE



**COMMANDEZ** SUR [CARREFOUR.FR](https://www.carrefour.fr)



TECHNOLOGIE

# Gigantesque cyberattaque inédite en cours contre "l'infrastructure d'internet"

LV 3949 FOIS | LE 23/02/2019 À 10:02 | ⌚ MIS À JOUR LE 23/02/2019 À 10:03 | [f](#) [t](#) [in](#) [✉](#)



**COM**



# L'affaire des chatons verts

## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,



## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,
- En général liés à des gouvernements au Moyen-Orient,

## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,
- En général liés à des gouvernements au Moyen-Orient,
- L'ICANN n'a pas été touchée (mais la racine, presque),

## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,
- En général liés à des gouvernements au Moyen-Orient,
- L'ICANN n'a pas été touchée (mais la racine, presque),
- Ce n'est pas une attaque DNS,

## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,
- En général liés à des gouvernements au Moyen-Orient,
- L'ICANN n'a pas été touchée (mais la racine, presque),
- Ce n'est pas une attaque DNS,
- Attaque remarquable par son ampleur, sa durée, son professionnalisme,

## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,
- En général liés à des gouvernements au Moyen-Orient,
- L'ICANN n'a pas été touchée (mais la racine, presque),
- Ce n'est pas une attaque DNS,
- Attaque remarquable par son ampleur, sa durée, son professionnalisme,
- Et le fait que plusieurs acteurs importants de l'Internet ont été piratés,

## L'affaire des chatons verts

- AttaqueS contre des noms de domaine, au moins de septembre à décembre 2018, médiatisée début 2019,
- En général liés à des gouvernements au Moyen-Orient,
- L'ICANN n'a pas été touchée (mais la racine, presque),
- Ce n'est pas une attaque DNS,
- Attaque remarquable par son ampleur, sa durée, son professionnalisme,
- Et le fait que plusieurs acteurs importants de l'Internet ont été piratés,
- Par contre, aucune innovation technologique.

# Outils d'investigation

## Outils d'investigation

- *Passive DNS* : récolte de réponses DNS



## Outils d'investigation

- *Passive DNS* : récolte de réponses DNS
- J'utiliserai DNSDB, le Web Archive du DNS.

## Outils d'investigation

- *Passive DNS* : récolte de réponses DNS
- J'utiliserai DNSDB, le Web Archive du DNS.
- Les journaux « ajout à la fin seulement » comme *Certificate Transparency* (RFC 6962), le Web Archive des certificats.

## Outils d'investigation

- *Passive DNS* : récolte de réponses DNS
- J'utiliserai DNSDB, le Web Archive du DNS.
- Les journaux « ajout à la fin seulement » comme *Certificate Transparency* (RFC 6962), le Web Archive des certificats.
- whois.

# Outils d'investigation

- *Passive DNS* : récolte de réponses DNS
- J'utiliserai DNSDB, le Web Archive du DNS.
- Les journaux « ajout à la fin seulement » comme *Certificate Transparency* (RFC 6962), le Web Archive des certificats.
- whois.
- Les rares articles publics sérieux.

## Outils d'investigation

- *Passive DNS* : récolte de réponses DNS
- J'utiliserai DNSDB, le Web Archive du DNS.
- Les journaux « ajout à la fin seulement » comme *Certificate Transparency* (RFC 6962), le Web Archive des certificats.
- whois.
- Les rares articles publics sérieux.
- Un sigle utile : OSINT (*Open Source Intelligence*).

# Les dégâts

## Les dégâts

- Changement des enregistrements A (piratage à l'hébergeur), souvent via la colle (piratage au BE).

# Les dégâts

- Changement des enregistrements A (piratage à l'hébergeur), souvent via la colle (piratage au BE).
- Dans les exemples DNSDB, bien faire attention au bailliage.



# Les dégâts

- Changement des enregistrements A (piratage à l'hébergeur), souvent via la colle (piratage au BE).
- Dans les exemples DNSDB, bien faire attention au bailliage.
- Changement des enregistrements NS.

# DNSDB à la recherche des chatons verts

```
;; bailiwick: gov.eg.  
;;      count: 3  
;; first seen: 2018-11-14 18:41:30 -0000  
;; last seen: 2018-11-14 20:05:40 -0000  
mail.mfa.gov.eg. IN A 188.166.119.57
```

```
;; bailiwick: jo.  
;;      count: 3  
;; first seen: 2018-12-14 06:57:17 -0000  
;; last seen: 2018-12-15 01:59:08 -0000  
gid.gov.jo. IN NS ns1.lcjcomputing.com.  
gid.gov.jo. IN NS ns2.lcjcomputing.com.
```

# Les chatons verts ont eu des certificats

← → × 🏠  Sectigo Limited [GB] | https://crt.sh/?q=mail.mfa.gov.eg

**crt.sh** Ident

Criteria Ident

Certificates	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ↑	<a href="#">Not Before</a>	<a href="#">Not After</a>	
	<a href="#">946136592</a>	2018-11-14	2018-11-14	2019-02-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">946138197</a>	2018-11-14	2018-11-14	2019-02-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">53831850</a>	2016-11-20	2016-11-17	2019-04-04	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc."
	<a href="#">38933843</a>	2016-10-02	2011-06-08	2014-06-05	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc."
	<a href="#">16624386</a>	2016-04-13	2016-04-10	2019-04-04	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc."
	<a href="#">16614469</a>	2016-04-13	2016-04-11	2019-04-04	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc."
	<a href="#">1056762</a>	2013-04-08	2013-04-03	2016-04-03	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc."

# Pourquoi les certificats ne protègent pas

## Pourquoi les certificats ne protègent pas

- Deux sortes de certificats : DV (vérification qu'on contrôle un domaine) et EV (vérification en théorie plus strictes),

## Pourquoi les certificats ne protègent pas

- Deux sortes de certificats : DV (vérification qu'on contrôle un domaine) et EV (vérification en théorie plus strictes),
- **Dès qu'on a pris le contrôle d'un domaine, on a tous les certificats qu'on veut.**

# Et DNSSEC ?

## Et DNSSEC ?

- DNSSEC protège si l'attaquant contrôle juste l'hébergeur DNS (l'attaquant ne peut pas modifier le DS),



## Et DNSSEC ?

- DNSSEC protège si l'attaquant contrôle juste l'hébergeur DNS (l'attaquant ne peut pas modifier le DS),
- DNSSEC ne protège pas si l'attaquant a attaqué le BE (il peut modifier le DS),

## Et DNSSEC ?

- DNSSEC protège si l'attaquant contrôle juste l'hébergeur DNS (l'attaquant ne peut pas modifier le DS),
- DNSSEC ne protège pas si l'attaquant a attaqué le BE (il peut modifier le DS),
- Sauf si l'attaquant ne connaît pas DNSSEC, ce qui est fréquent, ou est distrait (ce qui est fréquent), ou manque de temps (TTL),

## Et DNSSEC ?

- DNSSEC protège si l'attaquant contrôle juste l'hébergeur DNS (l'attaquant ne peut pas modifier le DS),
- DNSSEC ne protège pas si l'attaquant a attaqué le BE (il peut modifier le DS),
- Sauf si l'attaquant ne connaît pas DNSSEC, ce qui est fréquent, ou est distrait (ce qui est fréquent), ou manque de temps (TTL),
- DNSSEC protège si un serveur secondaire est piraté,

## Et DNSSEC ?

- DNSSEC protège si l'attaquant contrôle juste l'hébergeur DNS (l'attaquant ne peut pas modifier le DS),
- DNSSEC ne protège pas si l'attaquant a attaqué le BE (il peut modifier le DS),
- Sauf si l'attaquant ne connaît pas DNSSEC, ce qui est fréquent, ou est distrait (ce qui est fréquent), ou manque de temps (TTL),
- DNSSEC protège si un serveur secondaire est piraté,
- DNSSEC ne protège pas si l'utilisateur ne valide pas (Let's Encrypt utilise un résolveur validant, mais pas Comodo).

# Une faiblesse chez l'hébergeur DNS

# Une faiblesse chez l'hébergeur DNS

- Hébergeur GoDaddy, décembre 2018.

## Une faiblesse chez l'hébergeur DNS

- Hébergeur GoDaddy, décembre 2018.
- N'importe qui pouvait se créer un compte GoDaddy gratuit, puis configurer une zone DNS, sans aucune vérification.

## Une faiblesse chez l'hébergeur DNS

- Hébergeur GoDaddy, décembre 2018.
- N'importe qui pouvait se créer un compte GoDaddy gratuit, puis configurer une zone DNS, sans aucune vérification.
- Si le domaine était hébergé chez GoDaddy **et** que le titulaire légitime n'avait pas de configuration pour son domaine (*dangling domain*), l'attaque marchait.



# « Subdomain attack »

## « Subdomain attack »

- Principe : la victime crée un nom de domaine comme `experience.company.example` puis abandonne le projet mais laisse le nom,

## « Subdomain attack »

- Principe : la victime crée un nom de domaine comme `experience.company.example` puis abandonne le projet mais laisse le nom,
- L'attaquant loue une machine (AWS, Linode, OVH...) jusqu'à avoir la même adresse IP,

## « Subdomain attack »

- Principe : la victime crée un nom de domaine comme `experience.company.example` puis abandonne le projet mais laisse le nom,
- L'attaquant loue une machine (AWS, Linode, OVH...)  
jusqu'à avoir la même adresse IP,
- Variante : avec les CNAME (attaque contre Windows Tiles en avril 2019).

# Piratage d'un registre

## Piratage d'un registre

- .gr (Grèce) piraté en 10-24 avril 2019

## Piratage d'un registre

- .gr (Grèce) piraté en 10-24 avril 2019
- Le communiqué du registre rappelle « mais nous sommes ISO 27001 »

# Ministère des Affaires Étrangères


```
;; bailiwick: mfa.gr.  
;;      count: 9  
;; first seen: 2019-04-11 10:31:04 -0000  
;; last seen: 2019-04-11 12:06:50 -0000  
mail.mfa.gr. IN A 95.179.131.225
```





# Plan du tutoriel

- 1 Rappels rapides
- 2 DNSSEC
- 3 Piratage côté avitaillement
- 4 Dénis de service**
- 5 Vie privée
- 6 Conclusion


## Exemple







**Bert Hubert**  @PowerDNS\_Bert Follow 



By the way, it is not just you, many resolver operators are reporting large amounts of random queries for \*.s3.amazonaws.com, and this appears to be impacting performance here and there.

11:44 AM - 22 Oct 2019

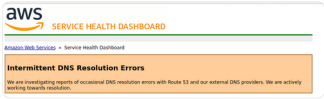
17 Retweets 21 Likes 

 5  17  21



**Bert Hubert**  @PowerDNS\_Bert · Oct 22 

Amazon now has this on [status.aws.amazon.com](https://status.aws.amazon.com): "Intermittent DNS Resolution Errors  
We are investigating reports of occasional DNS resolution errors with Route 53 and our external DNS providers. We are actively working towards resolution."







**aws** SERVICE HEALTH DASHBOARD


Amazon Web Services · Service Health Dashboard

**Intermittent DNS Resolution Errors**

We are investigating reports of occasional DNS resolution errors with Route 53 and our external DNS providers. We are actively working towards resolution.

 2  3  7



**shuLhan** @\_shuLhan · Oct 22 

Replying to @PowerDNS\_Bert

Oh, I thought it was just me. My small DNS server got hit since yesterday, with query type 46, 48, random S3 CNAME, and random qtype.

# Attaque « random QNAMEs »

## Attaque « random QNAMEs »

- Amazon Web Services, 22 octobre 2019

## Attaque « random QNAMEs »

- Amazon Web Services, 22 octobre 2019
- Plein de résolveurs (ouverts. . .) voient passer des requêtes de type CNAME pour \$RANDOM.s3.amazonaws.com

## Attaque « random QNAMEs »

- Amazon Web Services, 22 octobre 2019
- Plein de résolveurs (ouverts. . .) voient passer des requêtes de type CNAME pour \$RANDOM.s3.amazonaws.com
- Les serveurs faisant autorité ne répondent plus.

# Plan du tutoriel

- 1 Rappels rapides
- 2 DNSSEC
- 3 Piratage côté avitaillement
- 4 Déni de service
- 5 Vie privée**
- 6 Conclusion

# Vie privée



# Vie privée

- Le DNS en clair peut être espionné et modifié,

## Vie privée

- Le DNS en clair peut être espionné et modifié,
- DNSSEC protège contre la modification mais avec des limites,

# Vie privée

- Le DNS en clair peut être espionné et modifié,
- DNSSEC protège contre la modification mais avec des limites,
- Il faut chiffrer (RFC 7858, DNS-sur-TLS, et RFC 8484, DoH, DNS-sur-HTTPS),

# Vie privée

- Le DNS en clair peut être espionné et modifié,
- DNSSEC protège contre la modification mais avec des limites,
- 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).

# DoH

# DoH

- Pour chiffrer le DNS **du client final au résolveur**, on a DoT,

# DoH

- Pour chiffrer le DNS **du client final au résolveur**, on a DoT,
- Mais DoT utilise un port fixe, 853, trop facile à bloquer,

# DoH

- Pour chiffrer le DNS **du client final au résolveur**, on a DoT,
- Mais DoT utilise un port fixe, 853, trop facile à bloquer,
- D'où DoH (*DNS over HTTPS*) : port 443, plus difficile à bloquer.



# Polémiques sur DoH

## Polémiques sur DoH

- DoH ne permet plus de censurer. **Oui, c'est le but.**

## Polémiques sur DoH

- DoH ne permet plus de censurer. **Oui, c'est le but.**
- DoH ne permet plus de surveiller les requêtes. **Oui, c'est le but.**

## Polémiques sur DoH

- DoH ne permet plus de censurer. **Oui, c'est le but.**
- DoH ne permet plus de surveiller les requêtes. **Oui, c'est le but.**
- DoH aggrave la centralisation. **Ce n'est pas DoH, les résolveurs publics faisaient déjà cela. La solution : beaucoup de résolveurs DoH.**

## Polémiques sur DoH

- DoH ne permet plus de censurer. **Oui, c'est le but.**
- DoH ne permet plus de surveiller les requêtes. **Oui, c'est le but.**
- DoH aggrave la centralisation. **Ce n'est pas DoH, les résolveurs publics faisaient déjà cela. La solution : beaucoup de résolveurs DoH.**
- Le DNS fait partie du plan de contrôle du réseau et doit donc être géré par le FAI. **Je ne suis pas d'accord.**

## Polémiques sur DoH

- DoH ne permet plus de censurer. **Oui, c'est le but.**
- DoH ne permet plus de surveiller les requêtes. **Oui, c'est le but.**
- DoH aggrave la centralisation. **Ce n'est pas DoH, les résolveurs publics faisaient déjà cela. La solution : beaucoup de résolveurs DoH.**
- Le DNS fait partie du plan de contrôle du réseau et doit donc être géré par le FAI. **Je ne suis pas d'accord.**
- Tout sur HTTPS, c'est pas beau. **On n'a plus le choix.**

## Polémiques sur DoH

- DoH ne permet plus de censurer. **Oui, c'est le but.**
- DoH ne permet plus de surveiller les requêtes. **Oui, c'est le but.**
- DoH aggrave la centralisation. **Ce n'est pas DoH, les résolveurs publics faisaient déjà cela. La solution : beaucoup de résolveurs DoH.**
- Le DNS fait partie du plan de contrôle du réseau et doit donc être géré par le FAI. **Je ne suis pas d'accord.**
- Tout sur HTTPS, c'est pas beau. **On n'a plus le choix.**
- DoH fait faire la résolution DNS par l'application. **Faux (systemd, stubby).**

# Plan du tutoriel

- 1 Rappels rapides
- 2 DNSSEC
- 3 Piratage côté avitaillement
- 4 Déni de service
- 5 Vie privée
- 6 Conclusion**



## Les leçons à en tirer

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,
- Verrouillez vos domaines,

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,
- Verrouillez vos domaines,
- Superviser vos noms de domaines, pas juste le bon fonctionnement mais aussi le contenu.

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,
- Verrouillez vos domaines,
- Superviser vos noms de domaines, pas juste le bon fonctionnement mais aussi le contenu.
- Superviser les certificats émis pour vos domaines (par exemple avec Certstream).



## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,
- Verrouillez vos domaines,
- Superviser vos noms de domaines, pas juste le bon fonctionnement mais aussi le contenu.
- Superviser les certificats émis pour vos domaines (par exemple avec Certstream).
- Utilisez des VPN ou des résolveurs DNS chiffrés,

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,
- Verrouillez vos domaines,
- Superviser vos noms de domaines, pas juste le bon fonctionnement mais aussi le contenu.
- Superviser les certificats émis pour vos domaines (par exemple avec Certstream).
- Utilisez des VPN ou des résolveurs DNS chiffrés,
- Utilisez des résolveurs de confiance,

## Les leçons à en tirer

- Choisissez bien hébergeurs et BE, (facile à dire),
- Attention à l'ingénierie sociale,
- Signez vos zones avec DNSSEC,
- Utilisez un résolveur validant,
- Verrouillez vos domaines,
- Superviser vos noms de domaines, pas juste le bon fonctionnement mais aussi le contenu.
- Superviser les certificats émis pour vos domaines (par exemple avec Certstream).
- Utilisez des VPN ou des résolveurs DNS chiffrés,
- Utilisez des résolveurs de confiance,
- Utilisez des résolveurs avec minimisation des requêtes.