

*afnic*

# Détournement turc

*Stéphane Bortzmeyer*

*bortzmeyer@nic.fr*

*afnic*

*afnic*



# Le contexte

Le gouvernement turc est critiqué sur Twitter et YouTube...



# Le contexte

Le gouvernement turc est critiqué sur Twitter et YouTube...

... Il commence par demander aux FAI de censurer en configurant leurs résolveurs DNS pour mentir (21 mars)...



# Le contexte

Le gouvernement turc est critiqué sur Twitter et YouTube. . .

. . . Il commence par demander aux FAI de censurer en configurant leurs résolveurs DNS pour mentir (21 mars). . .

. . . Les utilisateurs passent à d'autres résolveurs, comme Google Public DNS. . .



# Le contexte

Le gouvernement turc est critiqué sur Twitter et YouTube. . .

. . . Il commence par demander aux FAI de censurer en configurant leurs résolveurs DNS pour mentir (21 mars). . .

. . . Les utilisateurs passent à d'autres résolveurs, comme Google Public DNS. . .

. . . Le gouvernement fait bloquer l'accès à ces résolveurs, cassant les connexions Internet (25 mars). . .

# Les faits

Les FAI turcs injectent des routes (29 mars) pour les gros résolveurs ouverts (8.8.8.8/32)...



# Les faits

Les FAI turcs injectent des routes (29 mars) pour les gros résolveurs ouverts (8.8.8.8/32)...

... Un serveur DNS est configuré pour répondre à ces adresses (comme 8.8.8.8). Il ment sur `twitter.com` et `youtube.com` pour envoyer vers 195.175.254.2...



# Les faits

Les FAI turcs injectent des routes (29 mars) pour les gros résolveurs ouverts (8.8.8.8/32)...

... Un serveur DNS est configuré pour répondre à ces adresses (comme 8.8.8.8). Il ment sur `twitter.com` et `youtube.com` pour envoyer vers 195.175.254.2...

**Ce n'est plus de la « simple » censure, c'est du piratage étatique.**

# Les preuves

- ① *Looking Glass* de Turk Telecom,
- ② Requêtes DNS à partir des sondes RIPE Atlas (si le réseau de la sonde est tunnelé à l'extérieur, le détournement disparaît),
- ③ Requêtes DNS par utilisateurs humains en Turquie,
- ④ Latence vers 8.8.8.8 mesurée par les sondes Atlas et par les sondes Renesys.

# Les solutions

DNSSEC aiderait... si les utilisateurs avaient un résolveur validant sur leur machine (la bonne solution)...

... Authentifier le résolveur (avec TSIG ou DNSCrypt - ce que fait OpenDNS) aiderait...

... RPKI n'y pourrait rien, le détournement étant interne. En fait, aucune solution de sécurité de routage n'aiderait...

... Pour l'utilisateur, les tunnels sont une solution.

*Merci !*

*afnic*

[www.afnic.fr](http://www.afnic.fr)  
[contact@afnic.fr](mailto:contact@afnic.fr)

*afnic*