Le Pakistan pirate YouTube

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 février 2008

http://www.bortzmeyer.org/pakistan-pirate-youtube.html

Ce dimanche 24 février, YouTube a été inaccessible depuis une bonne partie de la planète pendant une à deux heures. Ce n'était pas une panne, mais le résultat d'une action délibérée en provenance du Pakistan.

Un bon résumé de l'affaire peut être trouvé sur site de la BBC <http://news.bbc.co.uk/1/hi/technology/7262071.stm>. Le gouvernement du Pakistan a annoncé un blocage de YouTube <http://ap.google.com/article/ALeqM5gvcxE066Efob5tP2FP8ns9c0SNuwD8V0NK1G0>. Pakistan Telecom a exécuté l'ordre. Ce qui est intéressant, c'est que, incompétence, méchanceté ou bien volonté de tester, Pakistan Telecom a réussi à couper YouTube sur l'ensemble de la planète.

La technique employée est très banale et des tas de méchants l'ont déjà utilisée (le cas le plus célèbre est connu sous le nom d'AS 7007 <http://www.irbs.net/internet/nanog/9704/0378.html>). Elle se nomme « détournement d'adresse » ("*IP hijacking*") et consiste à annoncer une route plus spécifique, pour les adresses IP de la victime. Les routes sur Internet sont propagées d'opérateur en opérateur (par le protocole BGP, RFC 4271 [1]) et peu d'entre eux limitent ce qu'on peut annoncer. N'importe quel routeur BGP de l'Internet peut tout à coup se mettre à dire « Envoyez tous les paquets IP à destination de 208.65.153.0/24 - l'adresse de YouTube - vers moi ». Cette annonce aura même la priorité sur celle, légitime, de YouTube, car elle est plus spécifique (la longueur du préfixe est de 24 bits, contre 22 pour l'annonce légitime <http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRC001&query=1&arg=208.65.153.0> - notez qu'elle a changé depuis le détournement). Authentifier le pair BGP en face ne sert à rien, puisque cela ne garantit pas qu'il aura authentifié ses propres pairs (avec BGP, la confiance doit être transitive).

Quelles sont les leçons à en tirer ? L'insécurité de BGP est bien connue depuis longtemps et devrait, logiquement, susciter plus d'inquiétudes pour la sécurité et la stabilité de l'Internet que les débats politiciens de l'ICANN ou de l'IGF. Elle n'est pas facile à résoudre, le problème n'étant pas technique mais

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4271.txt

politique et organisationnel. Mikael Abrahamsson, qui travaille pour un opérateur suédois, a bien expliqué pourquoi personne ne filtre les annonces BGP (de manière très injuste, certains avaient reproché à PCCW, le fournisseur de Pakistan Telecom, son absence de filtrage) : « "*Using pure routing-registry based filtering just isn't cost efficient today, as these borks (unintentional mostly) we see sometimes are few and fairly far between, but problems due to wrong or missing information in the routing registries is plentyful and constant.*" » Bref (et c'est une leçon à retenir pour d'autres protocoles de sécurité comme DNSSEC), il y a plus de coupures si on protège que si on ne protège pas.

Ce ne sont donc pas les solutions techniques qui manquent (il y en a au moins deux, "*Secure BGP*" <http://www.ir.bbn.com/sbgp/> et soBGP <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html>) mais le modèle de confiance à déployer derrière. Pour prendre une comparaison, il ne sert à rien qu'un document d'identité soit infalsifiable si les services administratifs attribuent ces documents n'importe comment.

Si on veut éviter de se faire détourner ainsi, il n'y a guère de solutions, notons toutefois qu'il existe des services d'alerte <http://www.bortzmeyer.org/alarmes-as.html>, qui peuvent vous prévenir lorsqu'ils détectent une annonce de **votre** réseau par un nouvel opérateur : voir <http://www.ris.ripe.net/myasn.html> et <http://cs.unm.edu/~karlinjf/IAR/index.php>. Il est amusant de noter que ces services utilisent la même propriété que l'attaque <http://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html> : BGP est ouvert à tous, tout le monde peut y participer, tout le monde peut regarder (par exemple via les "*looking glasses*").

L'attaque (même si elle était involontaire, elle ne se distinguait pas d'une réelle attaque) a réactivé dans la communauté des opérateurs l'intérêt pour du filtrage politique (filtrer les opérateurs asiatiques et/ou musulmans) ou pour du filtrage économique (tout accepter des gros opérateurs et filtrer sévèrement les « petits », ceux qui n'ont pas YouTube pour client).

Cette attaque a été très médiatisée, puisqu'elle touchait une infrastructure critique de l'Internet : si on ne peut plus regarder des vidéos débiles tournées avec les pieds, la sécurité internationale est menacée. Trois semaines après, une bavure similaire a touché l'opérateur kenyan Africa on line et, là, cela n'a ému personne (voir un bon résumé de ce cas <http://asert.arbornetworks.com/2008/03/africa-online-kenya-latest-internet-routing-insecurity-casuality/>).

Trois très bons articles, sur des blogs de référence, résument la situation technique : <http://www.cs.columbia.edu/~smb/blog//2008-02/2008-02-24.html>, <http://www.potaroo.net/ispcol/2008-03/routehack.html>, et <http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml>. Une étude plus détaillée <http://www.ripe.net/news/study-youtube-hij html> a été faite par la suite par le RIPE-NCC, utilisant RIS, leur système de surveillance de BGP.

Sur BGP, on peut aussi lire mon cours pratique <http://www.bortzmeyer.org/deux-cours-routage.html>. Une solution technique à des problèmes de sécurité comme celui-ci a été normalisée en 2012, sous le nom de RPKI+ROA <http://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>.