Les drôles de pratiques BGP d'un opérateur bulgare et d'une université colombienne

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juin 2017

https://www.bortzmeyer.org/as-34991.html

Aujourd'hui, nous allons un peu regarder un drôle de problème BGP, et en n'utilisant que des sources ouvertes. L'infrastructure de l'Internet est en effet largement ouverte aux investigations.

Alors, d'abord, le premier fait : l'opérateur bulgare Wireless Network Solutions <http://www.wirelessnetbg.info/> annonçait en BGP un grand nombre de routes assez éloignées de ce qu'on attendrait de lui. L'annonce a cessé le 7 juin mais on peut toujours voir les anciennes annonces dans ce fichier issu de RIPE stat (en ligne sur https://www.bortzmeyer.org/files/as34991-ripestat.txt) ou directement sur RIPE Stat <https://stat.ripe.net/widget/announced-prefixes#w.resource=AS34991> :

Parmi les préfixes annoncés, on trouvait en effet des valeurs comme 168.176.219.0/24. Or, l'AS 34991 est situé en Bulgarie (ici, les données complètes (en ligne sur https://www.bortzmeyer.org/files/as34991-whois.txt), obtenues via whois). Alors que le préfixe 168.176.219.0/24 fait partie du 168.176.0.0/16 alloué à l'Université nationale de Colombie (ici, les données complètes (en ligne sur https://www.bortzmeyer.org/files/prefix168-176-whois.txt) via whois). Pourquoi donc un opérateur situé dans une petite ville de Bulgarie aurait-il comme client une université à Bogota ? Les liens économiques, historiques, linguistiques ou religieux, entre la Bulgarie et la Colombie semblent faibles. Creusons.

L'Université nationale de Colombie dispose d'un préfixe IPv4 de longueur 16 (cf. les données citées plus haut (en ligne sur https://www.bortzmeyer.org/files/prefix168-176-whois.txt)) mais ne l'annonce **pas** en BGP. On ne le voit pas sur RIPE stat <https://stat.ripe.net/widget/routing-status#w.resource=168.176.0.0%2F16>, ou sur le *"looking glass"* de Hurricane Electric <https://lg.he.net/>. Des sous-préfixes sont annoncés mais pas le /16 complet. Voyons sur RouteViews <http://www.routeviews.org/> en telnet :

```
% telnet route-views.routeviews.org
Trying 2001:468:d01:33::80df:3367...
Connected to route-views.routeviews.org.
...
User Access Verification

Username: rviews

route-views>show ip route 168.176.219.0
% Subnet not in table

route-views>show ip route 168.176.0.0
Routing entry for 168.176.0.0/16, 46 known subnets
  Variably subnetted with 7 masks
B        168.176.0.0/18 [20/0] via 66.110.0.86, 2d02h
B        168.176.64.0/19 [20/0] via 66.110.0.86, 2d02h
B        168.176.72.0/22 [20/0] via 66.110.0.86, 2d02h
B        168.176.76.0/24 [20/0] via 66.110.0.86, 2d02h
...
```

Donc, l'université colombienne n'annonce qu'une petite partie de son /16. À une époque où tout le monde souffre de la pénurie d'adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, c'est un peu curieux. L'annonce du sous-préfixe `168.176.219.0/24` par l'AS 34991 n'est donc **pas** un détournement BGP classique comme l'étaient ceux par Telekom Malaysia en 2015 <https://www.bortzmeyer.org/bgp-malaisie.html> ou bien lors du shunt de 2013 <https://www.bortzmeyer.org/bgp-shunt.html>. « Aucun préfixe BGP n'a été détourné pour le tournage de ce film. » Néanmoins, il ne semble pas non plus que cette annonce, qui n'a duré que dix jours, ait été légitime, à moins que le campus de Medell[Caractère Unicode non montré [1]]n n'ait eu envie pendant dix jours d'être connecté à l'Internet via la Bulgarie ? Une autre hypothèse, qui ne peut être formulée que par des gens pratiquant la méchanceté gratuite, serait que l'université a loué des /24 à des spammeurs bulgares…

Certains ont émis l'hypothèse que l'AS bulgare avait été pris par des méchants, à l'occasion d'une attaque flamant. Une attaque flamant est l'enregistrement d'un domaine qui n'existait pas, pour récupérer le courrier, y compris les demandes d'autorisation, d'un objet dont les contacts utilisaient des domaines disparus, ou mal enregistrés. Un exemple d'attaque flamant pour des TLD est par exemple documentée ici <https://thehackerblog.com/the-journey-to-hijacking-a-countrys-tld-the-hidden-risks/index.html>. La (je crois) première description publique date de 2007 <http://www.circleid.com/posts/help_domain_name_hijacked/>.

Les contacts techniques et administratifs de l'AS sont en `@wirelessnetbg.info`. Ils ont été modifiés juste avant les annonces bizarres, et le domaine créé peu de temps avant ces annonces (cf. les données récupérées par whois (en ligne sur `https://www.bortzmeyer.org/files/as34991-domain-whois.txt`), le champ "*Creation Date*"). Mais rien ne prouve (en tout cas avec des données ouvertes) qu'il y a eu une attaque flamant contre l'AS, bien qu'elle soit possible. Notez enfin que l'entreprise derrière l'AS ne semble pas exister dans le registre des entreprises en Bulgarie.

Merci à Ronald F. Guilmette pour avoir détecté le cas et l'avoir publié, et à Rayna Stamboliyska pour des investigations.

1. Car trop difficile à faire afficher par LaTeX