L'AS 13214 perd à nouveau la boussole

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 juillet 2009

https://www.bortzmeyer.org/as-13214-perd-boussole.html

Le protocole BGP est une source de distraction sans fin pour les administrateurs réseaux de l'Internet. Comme n'importe lequel des dizaines de milliers d'opérateurs Internet de la planète peut annoncer les routes qu'il veut, des incidents se produisent régulièrement. La plupart du temps, les différents filtres limitant la casse, puis les systèmes immunitaires de l'Internet <https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html> empêchent ces incidents de faire la une des journaux. Ce matin, c'est l'AS 13214 qui se signale à l'attention de tous, pour la deuxième fois en trois mois.

Vers 08h30 UTC, les utilisateurs du système d'alarme BGP <https://www.bortzmeyer.org/alarmes-as.html> Cyclops <http://cyclops.cs.ucla.edu/> reçoivent des messages inquiétants annonçant qu'un autre AS que leur leur annonce **leurs** préfixes IP :

```
Alert ID:                   5078076
Alert type:                 origin change
Monitored ASN,prefix:       192.134.4.0/22
Date:                       2009-07-28 08:30:26 UTC
No. monitors:               1
Announced prefix:           192.134.4.0/22
Announced ASPATH:           48285 13214
```

En clair, l'AS 13214 (DCP <http://dcpnetworks.com/>, en Suède) annonce des préfixes IP qui ne lui appartiennent pas, et ce en mettant son propre numéro d'AS dans le chemin BGP (ASPATH, qu'il faut lire de droite à gauche, le premier AS est le plus à droite). La lecture de la liste de diffusion Nanog <http://mailman.nanog.org/pipermail/nanog/2009-July/012227.html> montre vite que le problème est mondial : l'AS 13214 est en train d'annoncer toute la table de routage de l'Internet !

Le plus drôle est que le même AS avait fait la même bétise deux mois plus tôt <http://bgpmon.net/blog/?p=191>.

Mais, pas de panique : un seul des moniteurs de Cyclops a vu le problème (la ligne `No. monitors: 1`). Cela veut donc dire qu'il ne s'est pas propagé loin. Les autres systèmes d'alarme comme BGPmon `<http://bgpmon.net>` n'ont rien vu. Probablement, les filtres ont fonctionné dans la plupart des endroits.

Normalement, lorsqu'on échange en BGP avec quelqu'un, on n'accepte pas n'importe quoi de lui (sauf s'il s'agit de son fournisseur de transit). Au minimum, on limite le nombre de préfixes `<files/bgp.html#max-prefixes>`. Si on peut, on liste les préfixes que le pair BGP est autorisé à annoncer. Pourquoi Robtex `<http://www.robtex.com/>`, l'AS 48285 qui a relayé l'annonce erronée, ne le faisait-il pas, surtout après l'incident de Mai ? Parce que ce n'est pas facile : DCP est le fournisseur de transit de Robtex et on ne peut pas filtrer les annonces de son fournisseur, on est obligés de lui faire confiance.