Surveiller ses annonces BGP avec les systèmes d'alarme

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 mai 2009. Dernière mise à jour le 18 mai 2009

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

La sécurité du protocole BGP suscite régulièrement de l'intérêt, en général suite à des attaques spectaculaires comme celle de Pakistan Telecom contre YouTube <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>. En l'absence de mécanisme de signature cryptographique des annonces BGP (mécanisme très difficile à concevoir puisque les routeurs BGP, les préfixes IP et les AS ne forment pas un arbre mais un graphe très touffu), la seule protection contre les détournements est la vigilance <https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html>. Il existe plusieurs moyens automatiques d'être prévenus d'un changement d'annonces BGP et j'en teste ici quatre.

C'est dans le RFC 4271 [1] que BGP est normalisé. L'un des principes de base de BGP est que chaque routeur transmet **transitivement** des annonces de routes et que la confiance dans son pair BGP ne suffit pas, il faut aussi vérifier ces annonces, qui viennent parfois de loin. Comme il n'existe pas, même sur le papier, de mécanisme pour le faire, la seule approche raisonnable est de s'abonner à un ou plusieurs services d'alarme, comme IS (ex-MyASN) <https://www.ripe.net/is/alarms> ou BGPmon <http://www.bgpmon.net/>, testés ici. Ces systèmes préviennent même lors des attaques BGP les plus sophistiqués comme celle de Kapela & Pilosov <https://www.bortzmeyer.org/faille-bgp-2008.html>. (Cet article suppose une connaissance minimum de BGP donc il vaut peut-être mieux réviser un cours comme le mien <https://www.bortzmeyer.org/deux-cours-routage.html>.)

Comment fonctionnent ces systèmes d'alarme ? En exploitant justement ce qui fait la vulnérabilité de BGP, le fait que n'importe qui puisse s'y connecter. Le système d'alarme a donc un certain nombre de **points d'observation** où des routeurs BGP se connectent ("*peerent*") à un certain nombre d'opérateurs et reçoivent d'eux les mises à jour BGP. Cela permet de voir toutes les annonces BGP de la planète, et de détecter les changements, qui peuvent être le signe d'une attaque (ou d'une erreur de configuration). On peut alors signaler le changement, charge à l'administrateur réseau de décider s'il s'agit d'une fausse alerte ou pas (je vous préviens tout de suite, la complexité du réseau fait que les fausses alertes sont fréquentes, surtout si on ne connait pas bien son réseau).

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

Un système d'alarme qui n'aurait qu'un seul point d'observation serait sans doute insuffisant. En effet, il ne verrait pas tous les problèmes mais uniquement ceux qui l'atteignent. Par exemple, une attaque par usurpation n'atteindra pas un service mono-point d'observation (et ne sera donc pas signalée) si le routeur légitime est situé plus près. Il est donc préférable d'avoir un système distribué avec plusieurs points d'observation de BGP.

BGPmon <http://bgpmon.net/> est sans doute le plus simple et le plus efficace de ces systèmes d'alarme. On crée un compte sur le site Web et on indique les préfixes IP que l'on veut surveiller (rappelez-vous qu'il n'y a pas d'authentification du « responsable » d'un préfixe, on peut donc surveiller aussi ceux des concurrents).

Par exemple, je déclare que je veux surveiller 192.134.0.0/22. BGPmon m'indique automatiquement les annonces qu'il a déjà vu pour ce préfixe et me propose une liste d'AS qui l'ont annoncé dans le passé. Cela permet, même si on n'a pas de liste à jour de ses pairs BGP, d'éviter une longue période d'essais et d'erreurs. Il existe plusieurs options, comme la possibilité d'ignorer les préfixes plus spécifiques (une mauvaise idée, l'affaire YouTube utilisait justement un préfixe plus spécifique, de façon à ce que la route « pirate » soit préférée, IP choisissant la route la plus spécifique).

Normalement, bien sûr, chaque AS connait ses pairs et sa politique d'annonces, et la publie dans un IRR, au format RPSL (RFC 4012). Mais, dans le monde réel, ce n'est pas toujours le cas et le fait que BGPmon propose par défaut les annonces passées est bien pratique (quoique un peu dangereux s'il y avait une attaque dans ces annonces).

Une fois qu'il est ainsi configuré, BGPmon envoie un courrier électronique en cas d'annonce ne rentrant pas dans ce cadre (nouvel AS d'origine, ou bien AS de transit non listé) :

```
You received this email because you are subscribed to BGPmon.net.
For more details about these updates please visit:
http://bgpmon.net/showupdates.php

======================================================================
Change of upstream AS (Code: 31)
======================================================================
Your prefix:          192.134.0.0/22:
Update time:          2009-04-18 05:11 (UTC)
Detected by #peers:   1
Detected prefix:      192.134.0.0/22
Announced by:         AS2486 (NICFR-DNS-GIX-PARIS --  AFNIC)
Upstream AS:          AS15412 (FLAG-AS Flag Telecom Global Internet AS)
ASpath:               29073 24785 15412 2486
Mark as false alert:  http://bgpmon.net/fp.php?aid=21227935


----------------------------------------------------------------
 *for questions regarding the change code or other question, please see:
http://bgpmon.net/faq.php
```

On notera la possibilité de déclarer immédiatement qu'il s'agissait d'une fausse alerte (par exemple parce qu'on avait oublié un AS dans la liste), bien pratique. J'apprécie également le fait que les numéros d'AS soient automatiquement traduits en noms. On peut également voir les alertes sur sa page Web .

BGPmon est donc simple, facile à utiliser et efficace. Un autre système est Information Services (IS) <http://www.ripe.net/is/alarms/> (ex-myASN) du RIPE-NCC. Celui-ci repose sur les très nombreux points d'observation du RIS <http://www.ripe.net/ris/>.

Pour utiliser IS, on se crée un compte gratuitement sur le serveur du RIPE-NCC, et, comme avec BGPmon, on déclare ses préfixes. Je trouve l'interface nettement moins agréable qu'avec BGPmon, par exemple parce qu'il faut déclarer séparément les tests pour l'AS d'origine et les AS de transit et aussi parce qu'il n'existe pas d'auto-détection, utilisant les anciennes annonces.

Les alarms peuvent être envoyées par courrier ou bien par syslog. Les messages ressemblent à :

```
Subject: [RIPE NCC Alarm] AS 2486 transit
To: bortzmeyer+ripealarm@nic.fr
Date: Thu, 7 May 2009 00:15:43 +0000

The condition for your alarm 'AS 2486 transit' was triggered.

One of your "MyASN Monitor Transit" alarms was triggered based on the following conditions:

Prefix: 192.134.0.0/22
AS Path: 25152 23148 8928 2486
Neighbor of Origin: 8928 2486
Seen by Route Collector: 16
Peer IP: 198.32.124.146
Peer AS Number: 25152
Timestamp (GMT): 14:38, May 6 2009
```

Par rapport aux alarmes de BGPmon, on note l'identité du routeur qui a perçu le problème (ici le 16). Les alarmes peuvent aussi se voir sur l'interface Web :

Un autre service d'alarme est Cyclops <http://cyclops.cs.ucla.edu/>. Fondé sur des sources obtenues de nombreux routeurs, il permet également de configurer des alarmes et de les voir sur le site Web. Comme BGPmon, il a aussi une fonction d'auto-détection, pour remplir les informations originales. Voici un exemple de message d'alerte de Cyclops :

```
This message lists 1 out of a total of 1 alerts detected recently. You can mark each
alert bellow as a "false alert" so that you won't receive more alerts with the same
root-cause in the future.
To view all your alerts please go to: http://cyclops.cs.ucla.edu/?v=ma&tab=4

-------------------------------------------------
Mark as false alert (need to be logged in):
   http://cyclops.cs.ucla.edu?v=false_alert&uid=365&aid=3590692
Alert ID:                     3590692
Alert type:                   next-hop change
Monitored ASN,prefix:         192.134.0.0/22
Offending attribute:          192.134.0.0/22-174
Date:                         2009-05-18 08:15:35 UTC
Duration:                     00:00:01 (hh:mm:ss)
No. monitors:                 1
   (http://cyclops.cs.ucla.edu/view_monitors.html?aid=3590692)
Announced prefix:             192.134.0.0/22
Announced ASPATH:             3267 174 2486
BGP message:
   http://cyclops.cs.ucla.edu/show_myalert.html?aid=3590692
-------------------------------------------------
```

Le principal problème que je lui trouve est que le serveur Web est très lent.

Enfin, dernier service testé, le moins riche (mais sérieux, et qui marche), IAR <http://cs.unm.edu/~karlinjf/IAR/>. Il gère uniquement les AS, pas les préfixes. Voici un exemple des alarmes reçues :

```
Subject: [IAR] An alert from the Internet Alert Registry
From: IAR@cs.unm.edu
Date: Tue, 28 Apr 2009 06:32:34 -0600 (MDT)

AS 2200 is now announcing 134.206.0.0/16 which is historically
announced by ASes: 1725.
Time: Tue Apr 28 13:37:07 2009 GMT
Observed path: 812 1273 2200
...
```

On peut aussi explorer interactivement la table BGP du moment avec les looking glasses <http://www.traceroute.org/#LookingGlass> ou bien les serveurs de route <http://www.traceroute.org/#RouteServers> (attention, la plupart de connaissent que les routes locales, par exemple que celles de leur point d'échange). Et les annonces BGP récentes sont accessibles avec Routing Information Service <http://www.ripe.net/ris/index.html> ou bien BGP : :Inspect <http://bgpinspect.merit.edu/>. Parmi les autres systèmes d'alarme qui existent mais qui ne sont pas testés ici :

— Routing Intelligence <http://www.renesys.com/products_services/routing_intelligence/> de Renesys qui, à ma connaissance, n'a pas de version gratuite, même limitée,

Le mécanisme standard de validation cryptographique des annonces de route se nomme RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> et est, début 2012, encore très peu déployé.

Merci à Andree Toonk, l'auteur de BGPmon pour son aide et sa réactivité.