Détournement de préfixes et routage externe

Nous analysons dans ce document un évènement fréquent sur Internet qui consiste en un détournement de préfixes d'adresses IP. Nous considérons l'épisode qui a eu lieu le **6 novembre 2015**. Cet épisode a touché des milliers de préfixes appartenant à des entités différentes telles que *Cisco*, *FedEx*, *Toyota*, *Harvard*, ou *Associated Bank* sujet de cette étude.



Un préfixe d'adresses IP est un bloc d'adresses contiguës. Par exemple, 192.168.1.0/24 dénote l'ensemble des adresses IP comprises entre 192.168.1.0 et 192.168.1.255.

La banque *Associated Bank* dispose de huit préfixes d'adresses IP dont le préfixe 12.180.184.0/24 analysé ci-dessous. Ce préfixe est annoncé par BGP aux fournisseurs d'accès de la banque : *AT&T* et *Windstream*. A leur tour, *AT&T* et *Windstream* relayent l'annonce de préfixe de la banque vers *NTT* et *TeliaSonera*. Ainsi, de proche en proche, l'information de routage se propage pour atteindre tous les réseaux sur Internet comme indiqué sur la figure 1.

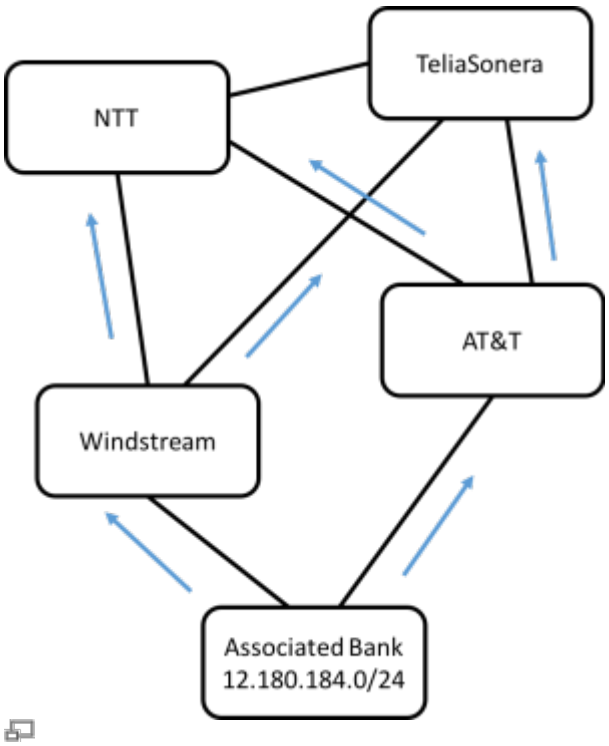


Figure 1. Annonces de routage

De cette façon, les routeurs BGP des différents réseaux sur Internet sélectionnent un chemin vers le réseau de la banque. Ils peuvent maintenant router le trafic vers le préfixe 12.180.184.0/24, comme représenté sur la figure 2. En particulier, le serveur qui héberge le site web de la banque associatedbbank.com et qui est identifié par l'adresse IP 12.180.184.143 devient joignable.

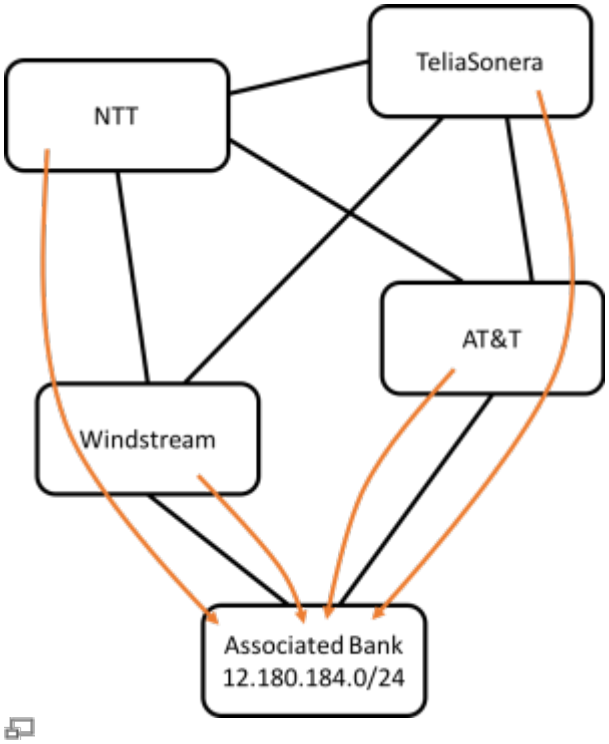
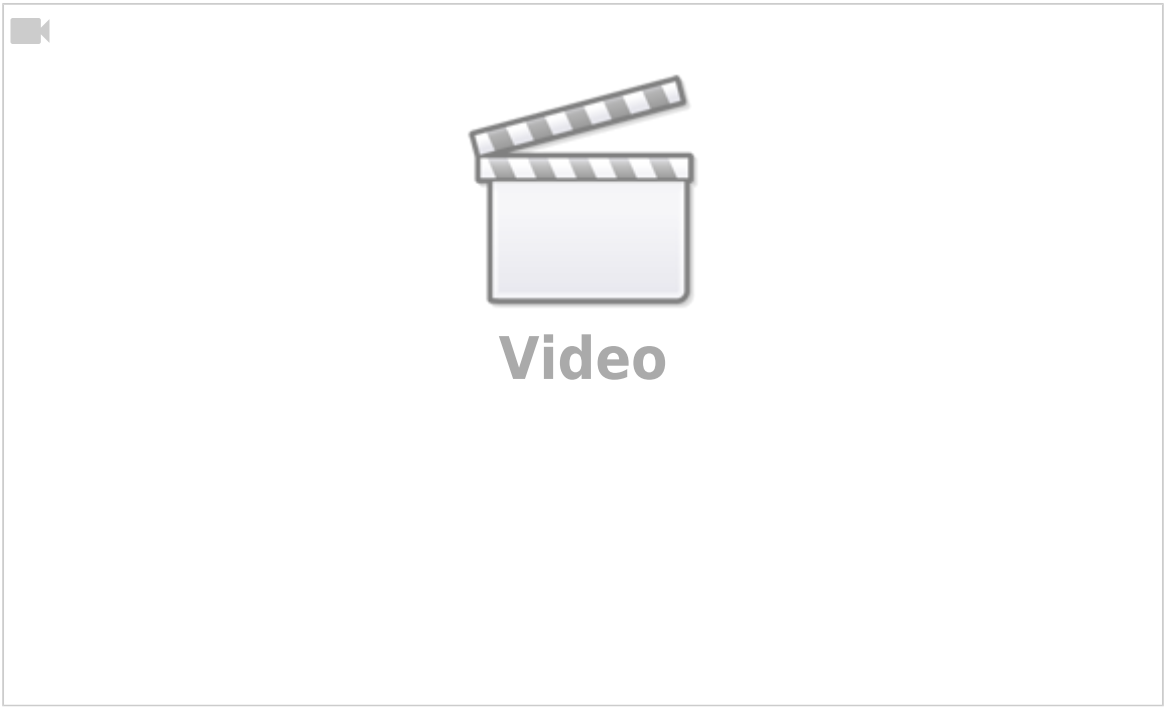


Figure 2. Acheminement du trafic

Mais que se passe-t-il si un autre réseau, dans cet épisode l'opérateur téléphonique indien *Airtel*, annonce par BGP qu'il possède le préfixe 12.180.184.0/24 ?



Pour cela, observons une capture vidéo de l'outil BGPlay déployé par RIPE NCC. Cet outil permet de suivre les informations de routage sur des sondes installées dans différents points du monde. Dans cette vidéo, les réseaux sont identifiés par les numéros de systèmes autonomes : par exemple, 14561 correspond à *Associated Bank*, 7018 à *AT&T*, 3356 à *Level 3*, et 9498 à *Airtel*.

Au début de la vidéo, le système autonome 14561 annonce le préfixe 12.180.184.0/24. Les sondes installées en Suisse (25091), en Grande Bretagne (3252), à Singapore (24482), ou en Russie (20632), sélectionnent des chemins vers le préfixe 12.180.184.0/24 qui passent par *AT&T* et aboutissent sur le réseau de la banque *Associated Bank* (représenté en rouge avec le numéro 14561).

A l'instant 00:04 sur la vidéo (ce qui correspond à 5h53 le 6-11-2015), le système autonome *Airtel* commence à annoncer le préfixe 12.180.184.0/24. Les systèmes autonomes 20632 et 9002 situés en Russie sélectionnent maintenant des chemins vers le préfixe de la banque qui aboutissent sur le réseau de l'opérateur indien !

Petit à petit, les annonces de l'opérateur indien se propagent. A l'instant 00:10, les systèmes autonomes en Suisse, Grande Bretagne, à Singapore, ou en Russie sélectionnent des chemins vers *Airtel*. Par conséquent, le trafic qui devait être routé vers *Associated Bank* est détourné vers *Airtel*.

Nous assistons donc à un détournement de préfixes d'adresses IP qui aboutit à détourner le trafic de la banque vers l'opérateur indien. A la fin de la vidéo, nous observons que le détournement s'arrête et le trafic converge comme prévu initialement vers le réseau de la banque.

Conséquences du détournement

Le détournement de préfixes d'adresse IP a généralement des conséquences directes sur le fonctionnement d'Internet :

- Le trafic n'est plus routé vers le système autonome qui possède le préfixe détourné.
- Les serveurs du système autonome qui possède le préfixe détourné ne sont plus joignables.
- Le système autonome qui a détourné le préfixe reçoit le trafic correspondant : il peut donc analyser son contenu (essentiellement pour le trafic qui n'est pas chiffré).
- Le système autonome qui a détourné un grand nombre de préfixes peut provoquer une congestion sur son infrastructure ou celle de son fournisseur.

Le détournement de préfixes IP dans l'actualité

Le problème de détournement de préfixe d'adresses IP est un problème connu sur Internet. Des épisodes célèbres comme le piratage de YouTube par Pakistan Telecom ont été très médiatisés. Le site bgpstream.com permet de suivre en temps réel l'occurence de tels évènements sur Internet. Ils sont marqués comme `Possible Hijack`.



Un détournement n'est pas nécessairement un acte malveillant, mais peut être le résultat d'une mauvaise configuration du routage BGP.

Existe-t-il des solutions à ce problème ?

La solution actuelle qui contribue à éviter le détournement de préfixes IP consiste à utiliser l'infrastructure RPKI. Un routeur BGP peut valider l'authenticité d'une annonce de routage à l'aide de certificats numériques. Comme indiqué dans l'exemple ci-dessous, le préfixe 12.180.184.0/24 n'est pas associé à un certificat qui permet de valider l'annonce de routage en provenance de la banque. Ceci aurait pu éviter le détournement par l'opérateur indien (à condition que les routeurs BGP qui reçoivent les annonces effectuent la validation). Contrairement, le préfixe 81.194.0.0/16 annoncé par

RENATER dispose d'un certificat associé. Tout routeur qui reçoit une annonce de ce préfixe peut procéder à la validation et potentiellement écarter une annonce mensongère ou baisser sa priorité.

```
$ whois -h whois.bgpmon.net 12.180.184.0/24

Prefix:              12.180.184.0/24
Prefix description:  Fiserv
Country code:        US
Origin AS:           14561
Origin AS Name:      Associated Bank
RPKI status:         No ROA found
First seen:          2011-10-19
Last seen:           2015-11-15
Seen by #peers:      217

$ whois -h whois.bgpmon.net 81.194.0.0/16

Prefix:              81.194.0.0/16
Prefix description:  FRANCE
Country code:        FR
Origin AS:           2200
Origin AS Name:      Reseau National de telecommunications pour la
Technologie
RPKI status:         ROA validation successful
First seen:          2011-10-19
Last seen:           2015-11-15
Seen by #peers:      224
```

Comme indiqué sur le site http://rpki-monitor.antd.nist.gov, l'utilisation de l'infrastructure RPKI est encore à ses débuts. Le routage externe basé le protocole BGP présente encore des failles qui rendent possibles des actes malveillants tels que le détournement de préfixes d'adresses IP.



- Identifiez et commentez des détournements de préfixes sur https://bgpstream.crosswork.cisco.com.
- Testez la validité des certificats numériques associés aux préfixes de votre choix sur https://rpki-validator.ripe.net/.

From:
https://wiki.lahoud.fr/ - **wikiroute**

Permanent link:
https://wiki.lahoud.fr/doku.php?id=detournement_de_prefixes

Last update: **2022/11/23 23:40**