Détournement de préfixes et routage externe

Nous analysons dans ce document un évènement fréquent sur Internet qui consiste en un détournement de préfixes IP. Nous considérons l'épisode qui a eu lieu le **6 novembre 2015** et concernait le préfixe de la banque *Associated Bank* située aux Etats-Unis.



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 qui est l'objet de cette étude. 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.

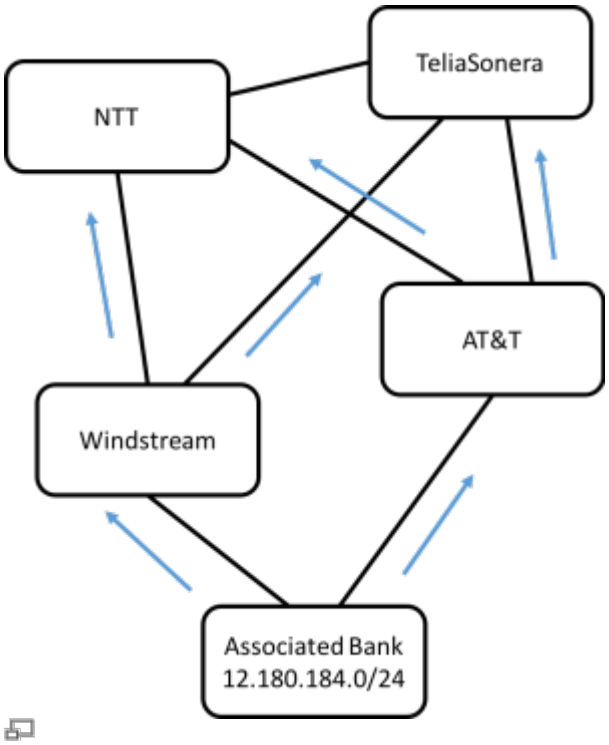


Figure 1. Annonces de routage

De cette façon, les routeurs BGP des différents réseaux sur Internet sélectionnent un chemin vers le réseau de la banque. Ils peuvent maintenant routeur du 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.

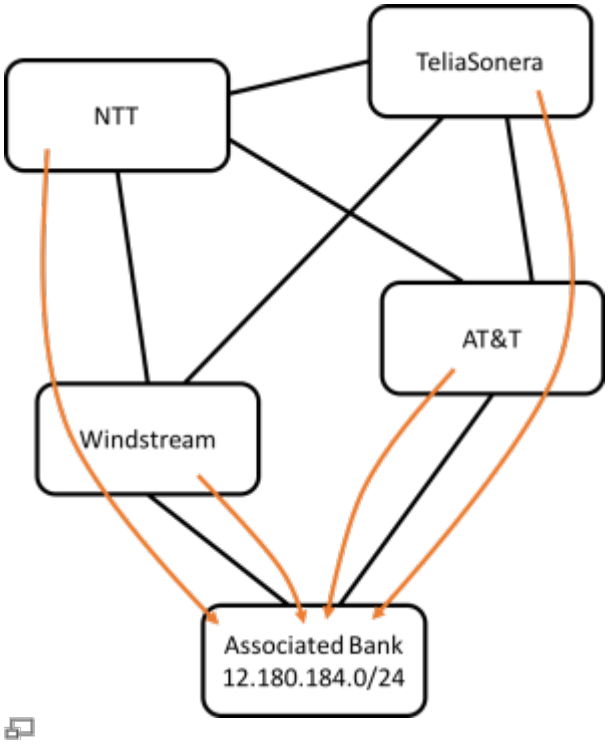
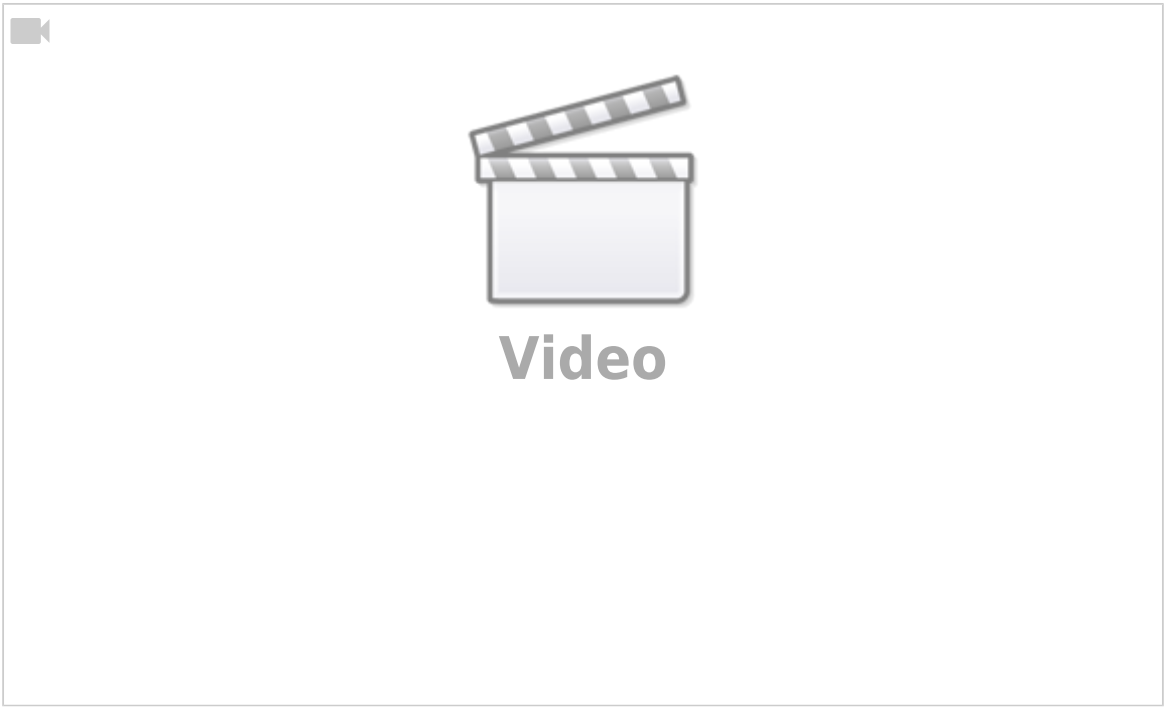


Figure 2. Acheminement du trafic

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 système autonome : 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 par exemple 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* pour aboutir sur le réseau de la banque *Associated Bank* (représenté en rouge avec le numéro 14561).

A la séquence 0:24 de la vidéo, 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 et à 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*.

Le problème est résolu à la fin de la vidéo et le trafic converge comme prévu vers le réseau de la banque.



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 ?

Le problème de détournement de préfixe IP est un problème très connu. Des épisodes célèbres comme le piratage de YouTube par Pakistan Telecom a été très médiatisé. Le site bgpstream.com permet de suivre en temps réel l'occurence de tels évènements sur Internet.

La solution actuelle qui permet d'éviter le détournement de préfixes IP consiste à utiliser des certificats qui permettent de vérifier l'authenticité d'une annonce de routage.

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

Permanent link:
http://wiki.lahoud.fr/doku.php?id=detournement_de_prefixes&rev=1447604217

Last update: **2015/11/15 17:16**