Sécurité des Points d'échanges : BGP et BCP

Arnaud Fenioux et Will van Gulik
afenioux@franceix.net
will.van.gulik@ip-max.net

FranceIX / IP-Max

Résumé Les opéateurs Internet utilisent le protocole BGP afin d'échanger leurs informations de routage. Bien qu'étant ancien et n'utilisant pas de mécanisme de sécurité fort, ce protocole a su évoluer et de nombreuses recommandations BCP (Best Current Practices) et RFC ont été rédigées. Cette soumission a pour but d'expliquer les risques les plus souvent rencontrés sur les points d'échanges (IXP), ainsi que de présenter les solutions existantes afin de s'en prémunir. Cette approche sera composée d'un volet théorique et pratique (sous forme de retours d'expériences) afin appréhender les problématiques de sécurité rencontrées par les opérateurs se raccordant a un IXP.

1 Introduction

Afin de comprendre les termes utilisés par la suite, il est conseillé de lire l'article *Influence des bonnes pratiques sur les incidents BGP* [5] présenté au SSTIC en 2012. Nous présenterons tout de meme brièvement le protocole BGP et les Points d'échanges dans cette introduction.

1.1 Le protocole BGP

Chaque opérateur désirant se connecter à Internet dispose d'un numéro d'AS (*Autonomous System Number*) unique, ainsi que de plages d'adresses IP attribuées par un RIR (*Regional Internet Registry*). Le RIPE est chargé de gérer l'attribution de ces ressources pour l'Europe.

Pour échanger ces informations de routage entre eux, les opérateurs utilisent le protocole BGP, chaque annonce BGP sera donc définie par au moins : un préfixe (numero de réseau), un AS-PATH (liste des AS traversés pour arriver jusqu'a la destination), un NEXT-HOP (adresse IP du routeur le plus proche pour acheminer le trafic vers la destination).

On parlera de *Transit* lorsqu'un opérateur paye un intermédiaire pour acheminer le trafic jusqu'à la destination. Et à contratio, de *Peering* lorsque deux opérateurs sont directement interconnectés entre eux pour échanger leur trafic. Le peering est généralement une accord gratuit, alors que le transit est payant.

1.2 Les points d'échanges

Les opérateurs souhaitant peerer entre eux doivent être directement interconnectés, soit par l'utilisation d'un cable réseau entre leurs routeurs, soit par l'intermédiaire d'un point d'échange (aussi appelé IXP).

Les interconnexions directes (PNI *Private Network Interconnections*) ne sont généralement utilisées que lorsqu'il y a besoin d'échanger beaucoup de trafic. En effet, au niveau opérationnel, cela nécessiste de dédier un port sur le routeur et de maintenir une liaison par peer (voisin).

S'interconnecter à un point d'échange permet de joindre de nombreux peers via une seule liaison, l'IXP se comporte comme un switch virtuel de niveau 2 (tous les voisins sont dans le même LAN/réseau).

2 Risques et contre-mesures

2.1 Static Routing

Un problème à envisager lorsque l'on est connecté sur un IXP est l'utilisation possible par certains de routes statiques.

Une fois connecté à un point d'échange chaque opérateur peut choisir de peerer avec les autres membres. Cela peut etre avec la totalité des membres si l'opérateur a une politique de peering ouverte, ou seulement une partie des membres si l'opérateur a une politique de peering selective. Ce choix s'effectue au cas par cas et selon des critères propres à chaque opérateur (critères politiques, techniques ou économiques) comme expliqué dans le livre *The Internet Peering Playbook* [3].

Un peer s'étant vu refuser une demande de peering peut aisément définir une route statique vers le routeur cet opérateur afin de forcer tout le trafic qui lui est destiné à aller directement chez lui. Cette technique peut être détectée par une analyse fine des statistiques NetFlow (ou IPFIX). L'attanquant perd alors une partie de la résiliance, car si la victime met en place un filtrage (uRPF strict, ou une ACL interdisant le trafic provenant de l'adresse MAC du routeur de l'attanquant) le trafic sera alors "blackholé", c'est à dire détruit.

Si le routeur de l'opérateur cible contient une full-table (toute les destinations de l'internet) et n'est pas correctement sécurisé, il est même possible de faire pointer une route par défaut vers ce routeur afin d'utiliser ses transitaires et obtenir un acces complet et gratuit à Internet. Cette technique plus grossière que la précédente est d'autant plus visible et risquée, et peut être facilement déjouée par la victime via l'utilisation de VRF, d'une prefix-list qui n'accepte que le trafic à destination de son

propre réseau ou en s'assurant que le routeur connecté au point d'échange ne possède qu'un nombre limité de routes dans sa table de routage.

Tous ces mécanismes de protection sont expliqués dans la *BCP84* [4].

2.2 BGP Hijacking et MITM

Un des incidents le plus fréquemment vu sur Internet est le leak de routes et l'usurpation de préfixes (annonce non autorisée). Cela est généralement dû à une erreur de configuration et est corrigé dans les heures qui suivent, mais il arrive que cela soit fait dans un but précis : soit pour annoncer des plages IP non utilisées afin d'envoyer du spam, ou détourner du trafic afin de l'analyser ou d'en tirer un bénéfice pécunaire.

Tous ces mécanismes de protection sont expliqués dans le draft IETF *BGP operations and security* [2] ainsi que dans le guide des *Bonnes pratiques de configuration de BGP* [1] rédigé par l'ANSSI.

- next-hop hijacking (3 pfx) : annoncer un prefix vers quelqu'un d'autres - filtrage des RS & peer (as-set + rpki) https ://github.com/job/bgpq3 - martians filtering (team cymru)

Encore une raison de faire attention a ce qui est annoncé par ses peers. On a plusieurs fois entendu parlé de Prefix Hijacking. Ceci revient à annoncer un prefix qui ne nous appartient pas afin de pouvoir récupérer le trafic à des fins diverses (Vol de mot de passe, de bitcoin etc). Un cas récent était celui d'un des plus gros pool de bitcoin, Le prefix en question à été réannoncé ailleurs, de sorte à ce que les utilisateurs qui recevait l'annonce minent les bitcoins vers la nouvelle ip. Un moyen très efficace de voler des bitcoins, dans la mesure ou il était difficile d'identifier que l'ip contactée n'était pas au bon endroit, sans de plus conséquents analyse.

Un autre cas plus ancien est le fameux hijacking du prefix de youtube en 2008, par pakistan telecom. Dans ce cas, le but était, suite a une demande du gouvernement, d'empecher l'accès a Youtube. Le fournisseur de Pakistan Telecom à réannoncé ceci sans filtrage, et du coup une bonne partie du trafic pour youtube finissait chez pakistan telecom. On peut imaginer que ce n'est pas des petites quantités. http ://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/

D'ailleurs, il y a un grand nombre de Route-serveurs qui ne font aucun filtrages des annonces BGP, c est aussi a aborder je pensais.

2.3 DDoS URPF

Urpf + rtbh md5 et reset de sessions bgp

2.4 DoS BGP TCAM et ré-annonce

- max-prefix (trouver un 7600 lui annoncer plein de /24 cramer la rib en face) - 7600 et la tcam - spoofer une source et envoyer un packet ailleurs –> URPF : (en mode strict ca sauve la vie, en souple le spoofing passe) - Réannoncer le range de l'IXP en more specific (example de AMS-IX lors de la migration) –> Generalized TTL Security Mechanism (GTSM) rfc3682 - Spoofer l'IP d'un peers sur un IXP et envoyer beaucoup de RST a ses peers –> password MD5 sur le session

Ou c'est que certains croient, ou pire n'ont même pas constaté. Sur les routeurs Cisco, avec Sup720 3BXL ou RSP720, la tcam (mémoire utilisée pour adresser les IP) est configurable par software. La configuration par défaut est de 512k pour les routes IPv4. Au début de l'année 2014 la table de routage, selon où on se trouve sur le net, était d'environ 480k routes. En mi-aout de l'année 2014, un pic sur la quantité de route annoncée a fait passer la table à plus de 512k, affectant ces routeurs. L'effet est que les nouvelles updates de routes ne se font plus, et que la table ne peut pas plus grandir. Cela n'affecte en revanche pas le reste du fonctionnement du routeur. A ce moment certaine portion d'internet ne sont plus joignable. Une partie des utilisateurs de ces routeurs ont juste reloadé leur équipement et le problème a disparu, dans la mesure ou le pique était temporaire. Actuellement, les transitaires qui ne manipulent pas trop leur table de routage vont vous envoyer environ 510-520k routes (valeur du 22 janvier). Suggestions, si vous avez ces équipements modifiez vos Tcam (http ://www.potaroo.net/presentations/2014-05-12-bgp2013.pdf)

2.5 Risques lié a un IXP

- RA en v6 (d'ou la quarantaine et l'utilité sur les ixp) - multicast a checker (c'est filtré ou pas) possibilité de faire 100% des CPU Les pacquets IPv6 Router Advertisement sont monnaie courrante sur les IXP, car certains constructeurs active cette feature par défaut, et peu de tech le savent (ou s'en pré-occupent). Encore une fois, ce n est pas un truc super fun genre "hacking mega compliqué" mais ca ne devrait pas etre la.

-Drop sessions BGP -> MD5

2.6

2.7

3 Conclusion

Cet article a permis de dresser une liste non exaustive des risques rencontrés par un opérateur se raccordant à un point d'échange ainsi que de montrer les contre-mesures existantes. Nous avons pu constater que même si une bonne configuration de BGP sur son routeur permet de se prémunir des attaques les plus communes, il est aussi important d'activer des mécanismes de filtrages et de protection non directement relatifs à BGP.

Bien que ces mécanimes soient définis publiquement, implémentés et documentés depuis de nombreuses années, il est a noter qu'encore trop peu d'anministrateurs réseaux les mettent en place. Cela peut etre expliqué par le manque de temps, la non connnaissance de ces risques et moyen de s'en protéger, mais aussi que ces risques sont trop souvents considérés comme pas assez important pour s'en occuper.

Références

1. ANSSI. Bonnes pratiques de configuration de bgp. `http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_configuration_BGP.pdf`, 2013.
2. Jerome Durand Ivan Pepelnjak Gert Doering. Bgp operations and security. `https://tools.ietf.org/html/draft-ietf-opsec-bgp-security`, 2012. Internet Draft, Internet Engineering Task Force.
3. William B. Norton. The internet peering playbook. `http://drpeering.net/core/bookOutline.html`, 2012.
4. F. Baker P. Savola. Ingress filtering for multihomed networks. `https://tools.ietf.org/html/bcp84`, 2004.
5. François Contat Sarah Nataf Guillaume Valadon. Influence des bonnes pratiques sur les incidents bgp. `https://www.sstic.org/media/SSTIC2012/SSTIC-actes/influence_des_bonnes_pratiques_sur_les_incidents_b/SSTIC2012-Article-influence_des_bonnes_pratiques_sur_les_incidents_bgp-contat_valadon_nataf_2.pdf`, 2012. SSTIC.