RFC 7999 : BLACKHOLE Community

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 octobre 2016

Date de publication du RFC : Octobre 2016

https://www.bortzmeyer.org/7999.html

Lorsqu'on est soumis à une sérieuse attaque par déni de service volumétrique, il faut parfois sacrifier la machine qui en est la cible, afin de préserver le reste des ressources réseau. On demande alors à son opérateur de jeter le trafic à destination de cette machine, avant qu'il n'emprunte la liaison qu'on veut préserver. Cela peut se faire manuellement mais c'est évidemment plus rapide et moins risqué si on le fait automatiquement, via une annonce BGP vers le préfixe visé. Pour cela, on marque l'annonce BGP avec une **communauté** (RFC 1997[1]) qui veut dire « poubelle donc tout ce trafic ». Ce nouveau RFC normalise une communauté standard, « bien connue », pour cela, BLACKHOLE (0xFFFF029A). Ainsi, il n'y aura plus besoin d'utiliser une communauté différente pour chaque opérateur.

Cette méthode consistant à envoyer le trafic destiné à la victime vers un « trou noir » ("*blackholing*") est décrite dans les RFC 3882 et RFC 5635. Comme elle agit au niveau IP, elle ne nécessite pas d'équipements spéciaux, et elle est très rapide, ne prenant que peu de ressources chez les routeurs. Par contre, elle est peu subtile : tout le trafic à destination d'un préfixe donné (préfixe en général réduit à une seule adresse IP, celle de la machine attaquée) est jeté, qu'il fasse partie de l'attaque ou pas. Quel est l'intérêt de couper tout le trafic ? Cela réalise l'objectif de l'attaquant, non ? C'est en effet une mesure désespérée mais rationnelle : son but est de préserver les ressources réseau pour que les autres machines fonctionnent. Si vous êtes connecté à l'Internet par une liaison à 10 Gb/s, et qu'une attaque de 20 Gb/s frappe votre opérateur, votre ligne va être complètement inutilisable. Aucune action de votre côté n'y changerait rien, dès que les paquets sont arrivés chez vous, c'est trop tard. Ce RFC traite le cas où on demande à l'opérateur de jeter le trafic avant qu'il ne soit envoyé sur la ligne entre l'opérateur et vous.

Le problème (section 1 du RFC) est qu'il existait plusieurs méthodes pour déclencher cet envoi dans un trou noir, ce qui compliquait la tâche des équipes réseau, une annonce BGP marquée avec une certaine communauté, une annonce BGP avec un certain "*next hop*", et des méthodes non-BGP (dont le coup de

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1997.txt

téléphone au NOC). D'où la solution de notre RFC, définir une communauté standard. Plus besoin de se poser de question (à part celle de savoir si votre opérateur accepte cette commande, voir les sections 3.3 et 4). Au passage, les communautés BGP sont décrites dans le RFC 1997.

Une communauté BLACKHOLE est donc définie (section 2) et mise dans le registre IANA <https://www.iana.org/assignments/bgp-well-known-communities/bgp-well-known-communities.xml#bgp-well-known-communities-1> des communautés bien connues. Sa valeur est 0xFFFF029A. Le 666 à la fin vient de la Bible et était déjà couramment employé par les opérateurs. Notez donc que ce RFC n'invente pas une nouvelle technique (demander à son pair de jeter certains paquets est une technique très ancienne), il lui donne juste une communauté standard.

Voilà, c'est tout, juste une réservation d'un nom et d'une valeur. Si vous êtes intéressés par les détails pratiques, la section 3 est consacrée aux problèmes opérationnels. D'abord, un point essentiel : accepter des annonces BGP étiquetées BLACKHOLE est un choix local. Aucun opérateur n'est obligé de respecter cette demande et, dans ce cas, ladite communauté est ignorée. Lorsqu'on se connecte à un nouveau pair BGP, il peut donc être prudent de lire leur documentation ou de leur poser la question. N'utilisez BLACKHOLE qu'entre des adultes consentants. (Notez que cet avertissement du RFC est un peu contradictoire avec l'avantage proclamé de la normalisation de BLACKHOLE : en pratique, on est toujours obligé de savoir ce que fait son pair, on ne peut pas compter sur une méthode standard qui marcherait partout.) Une liste des opérateurs et points d'échange qui acceptent BLACKHOLE est disponible en ligne <https://github.com/tking/BLACKHOLE-BGP-Community>.

Si tout le monde accepte BLACKHOLE, on s'en sert comment ? Lorsqu'une attaque DoS est en cours, on annonce un préfixe qui couvre l'adresse IP visée, et on y ajoute cette communauté. On peut aussi utiliser BLACKHOLE pour les annonces du RFC 5635 (mais pas avec celles du RFC 5575).

Attention à ne pas propager ces annonces ! En effet, étant en général très spécifiques (souvent une seule adresse IP), elles seraient préférées, si elles étaient insérées dans une table de routage. Leur effet est prévu pour être strictement local et, donc, les annonces doivent être marquées avec la communauté NO_EXPORT (ou NO_ADVERTISE).

En parlant de spécificité, quelle doit être la longueur des préfixes annoncés avec un BLACKHOLE attaché ? Souvent, l'attaque ne vise qu'une seule adresse et, donc, les annonces BLACKHOLE seront souvent des /32 (en IPv4) et /128 (en IPv6), afin de ne sacrifier que le strict minimum de son réseau. Si vous avez une politique BGP de n'accepter que des préfixes plus généraux, c'est un point à modifier. Aujourd'hui (RFC 7454, section 6.1.3), les préfixes plus spécifiques que /24 (IPv4) et /48 (IPv6) sont rarement acceptés. Il faut donc faire des exceptions pour les trous noirs.

Lorsqu'un opérateur reçoit une de ces annonces « envoie-moi tout ça dans un trou noir », que doit-il vérifier ? Comme le résultat de cette annonce est de jeter tout le trafic, une attaque avec une annonce mensongère, ou bien une erreur d'un opérateur maladroit, pourrait avoir de sérieuses conséquences. Notre RFC recommande donc un certain nombre de tests de vraisemblance : vérifier que le pair est autorisé à annoncer un préfixe couvrant celui qu'il annonce avec BLACKHOLE, et vérifier que BLACKHOLE avec ce pair a été spécifiquement permis (le RFC recommande plus loin que ce ne soit pas permis par défaut). Même chose s'il y a des serveurs de route (RFC 7947) sur le trajet.

Par contre, il faut, pour le cas spécifique des annonces BLACKHOLE, débrayer les techniques de validation comme celle du RFC 6811. Par exemple, si un ROA ("*Route Origin Authorisation*", RFC 6482) autorise une longueur maximale de préfixe de /48, l'annonce BLACKHOLE de longueur /128 doit quand même être acceptée.

À des fins de traçabilité, pour faciliter l'analyse a posteriori d'une attaque, et du traitement qu'elle a reçu, le RFC recommande de journaliser toutes les annonces `BLACKHOLE`. (Cela permettra, par exemple, de repérer les pairs qui abusent du mécanisme, cf. section 6.)

Si vous travaillez chez un éditeur de logiciels pour routeurs, n'oubliez pas les conseils de la section 4, destinés aux programmeurs. D'abord, l'acceptation des annonces « trou noir » ne devrait pas être faite par défaut. Le RFC demande qu'une action explicite de l'administrateur réseau soit nécessaire. D'autre part, pour ne pas avoir à taper la valeur numérique de cette communauté, le RFC suggère de permettre une valeur texte à indiquer, par exemple `blackhole`.

Quelques petits points sur la sécurité pour finir (section 6). D'abord, bien se rappeler que BGP n'a par défaut aucun mécanisme pour empêcher ou détecter les modifications des annonces. Si un attaquant actif retire ou ajoute la communauté `BLACKHOLE`, ça ne se voit pas. Même le futur BGPSec ne l'empêchera pas, puisqu'il ne protège pas les communautés. Il y a donc des possibilités d'attaques par déni de service de ce côté.

C'est entre autre pour cela que le RFC demande qu'on vérifie qu'un pair qui annonce un préfixe avec `BLACKHOLE` est autorisé à le faire (RFC 7454, section 6.2.1.1.2).