RFC 6666 : A Discard Prefix for IPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 août 2012

Date de publication du RFC : Août 2012

https://www.bortzmeyer.org/6666.html

Une technique couramment utilisée en cas d'attaque par déni de service est le **RTBH** : "*Remote Triggered Black Hole*" où la victime demande à son FAI, via un protocole, de jeter des paquets sur tel ou tel critère. On utilise pour cela les protocoles de routage standards comme BGP ou OSPF. Même chose lorsqu'un opérateur réseaux veut propager en interne, entre ses routeurs, la décision de jeter ou de rediriger tel ou tel type de paquets. Pour cela, il est bien pratique de disposer d'un préfixe IP spécial, qui désigne le trou noir (ou l'IDS, si on redirige le trafic vers un équipement d'analyse spécial). Il n'existait pas de tel préfixe pour IPv6, c'est désormais fait avec ce RFC, qui enregistre `0100::/64`.

Les RFC 5635[1] et RFC 3882 décrivent plus en détail cette idée de RTBH dans le cas d'une DoS. On sélectionne les paquets en fonction de leur adresse IP source ou destination et on les jette (trou noir) ou bien on les envoie (par exemple via un tunnel) vers un dispositif d'analyse. Pour configurer cela, il faut des adresses IP (plusieurs, car on peut avoir plusieurs traitements différents selon les attaques, donc une seule adresse IP ne suffit pas). Certains utilisent des adresses privées ou bien les adresses IP réservées pour la documentation (RFC 3849). Ce n'est pas très satisfaisant (et cela peut interférer avec les politiques de filtrage en interne, cf. section 2 du RFC) d'où le nouveau préfixe. Si on voit `0100::/64` dans la configuration d'un routeur, on sait désormais exactement ce que cela implique.

Ce préfixe peut être propagé, à l'intérieur du réseau de l'opérateur, ou bien entre l'opérateur et ses clients, par les protocoles de routage dynamiques habituels comme OSPF. Il ne doit pas être transmis à l'extérieur et il est recommandé de le filtrer en entrée, sur les liens de "*peering*" ou de transit. Comme il sert pour gérer des attaques qui peuvent être de taille impressionnante, une fuite de ce préfixe vers un autre opérateur pourrait potentiellement entraîner un reroutage de l'attaque vers cet autre opérateur (sections 3 et 5 du RFC). Prudence, donc !

Ce préfixe `0100::/64` est désormais dans le registre des adresses IPv6 spéciales <https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xml>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5635.txt