RFC 6018 : IPv4 and IPv6 Greynets

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 septembre 2010

Date de publication du RFC : Septembre 2010

https://www.bortzmeyer.org/6018.html

Il y a longtemps que les chercheurs en sécurité des réseaux utilisent des "*darknets*", des réseaux dont les adresses IP ne sont normalement pas attribuées, pour analyser les attaques. Si on annonce une route vers un tel réseau, le trafic qu'on capte est essentiellement composé d'attaques ou de reconnaissances préalables à une attaque puisque rien de légitime ne peut utiliser ces réseaux. L'inconvénient des "*darknets*" est qu'ils sont trop gros et trop visibles : les attaquants apprennent vite leur existence et les mettent alors sur leur liste « pas touche » et les attaques cessent. Ce RFC décrit une alternative, le "*greynet*", dont le préfixe IP est alloué et routé mais au sein duquel certaines adresses ne correspondent pas à une machine en activité.

Normalement, un routeur IP doit jeter les datagrammes destinés à une adresse qui ne répond pas aux requêtes ARP (RFC 826 [1]) ou ND (RFC 4861). On pourrait envisager de configurer des règles spéciales par adresse IP, pour copier les datagrammes destinés à ces machines vers la sonde d'observation. Mais, pour construire facilement le "*greynet*", le RFC suggère une autre méthode : configurer le routeur pour que, au lieu de jeter les paquets qui ne peuvent pas être délivrés, il les copie vers la machine de surveillance. Toute adresse IP non affectée devient alors membre du "*greynet*".

On peut ainsi détecter les attaques (ou les reconnaissances) vers ces adresses, mais aussi les cas d'usurpation de ces adresses par un tiers. Ces usurpations vont en effet produire du "*backscatter*", de l'émission par les cibles en réponse aux reconnaissances, et une partie au moins de ce "*backscatter*" atteindra le "*greynet*".

La section 2 sert ensuite de manuel pour l'administrateur réseaux qui voudrait déployer un tel système. Il doit évidemment d'abord mettre en place la machine de collecte, qui va recevoir les paquets, les enregistrer et plus tard les analyser. Ensuite, il peut utiliser le routage IP normal et choisir

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc826.txt

un préfixe non utilisé pour le router vers cette machine, créant ainsi un "*darknet*" (section 2.1). Sur Linux, par exemple, cela se ferait avec `route add -net 192.0.2.128/25 gw 198.51.100.1` où `192.0.2.128/25` est le préfixe du "*darknet*" et `198.51.100.1` l'adresse de la machine de collecte.

Mais s'il veut faire un "*greynet*", il lui faut un routeur un peu spécial (section 2.2) qui va devoir, lorsqu'il reçoit un paquet pour lequel il n'a pas eu de réponse aux requêtes ARP et ND, le faire suivre à la machine de collecte. C'est à la fois plus simple qu'un "*darknet*" (pas de configuration explicite, à part l'adresse de la machine de collecte, cf. section 3) et plus compliqué (aucun routeur IP normal ne sait faire cela : en cas de non-réponse à ARP et ND, le paquet est abandonné).

La première documentation des "*greynets*" était dans « "*Greynets : a definition and evaluation of sparsely populated darknets*" <http://www.acm.org/sigcomm/sigcomm2005/paper-HarArm.pdf> », dans la "*30th Conference on Local Computer Networks*" de l'IEEE en 2005. Elle a été suivie de plusieurs expériences, résumées dans la section 1.1 du RFC. L'utilisation du routeur pour identifier les adresses du "*greynet*" (ce sont celles qui ne répondent pas en ARP ou en ND) est venue après. La première mise en œuvre était sur un routeur Linux. Le fichier à récupérer est <http://www.owenstephens.co.uk/files/neigh_fwd.c>, et il se place dans le répertoire `net/core` des sources du noyau. Il faut ensuite appeler les fonctions nécessaires depuis `neighbour.c`, le moyen le plus simple étant sans doute de "*patcher*" ce dernier avec <http://www.owenstephens.co.uk/files/neighbour.c.diff>. (Merci à Owen Stephens pour avoir mis les sources en ligne.)

L'ajout d'IPv6 est venue encore ultérieurement. Bien qu'on entende souvent dire qu'un balayage complet d'un réseau IPv6 est impossible, vu le nombre d'adresses possibles, le RFC 7707 a montré que c'était faux. En pratique, les attaques IPv6 n'ont jamais été observées dans la nature mais il ne fait guère de doute que cela se produira un jour.

Un dernier avertissement pour ceux qui veulent tenter l'aventure : lisez bien la section 6 sur la sécurité. Tout dispositif de collecte peut faire l'objet d'abus, par exemple par un méchant qui, sachant qu'une collecte est en cours, va tenter de la saturer en envoyant plein de paquets.