RFC 6305 : I'm Being Attacked by PRISONER.IANA.ORG!

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 juillet 2011

Date de publication du RFC : Juillet 2011

https://www.bortzmeyer.org/6305.html

Un RFC très inhabituel, non seulement par son titre amusant mais aussi parce que le public visé n'est pas le programmeur qui va mettre en œuvre des normes, ni même l'administrateur réseaux qui s'occupe de grands réseaux complexes, mais un public bien plus large, celui des gens qui gèrent un petit réseau, ont installé comme pare-feu ou IDS une boîte noire à laquelle ils ne comprennent rien, et qui voient arriver des messages d'alerte comme quoi leur petit réseau serait attaqué par un mystérieux `prisoner.iana.org`. Ce RFC a été écrit pour fournir à l'IANA et aux opérateurs de serveurs de l'AS112 (décrit dans le RFC 7534 [1]) une réponse toute faite à envoyer à ces angoissés.

En effet, l'« attaque » en question n'est pas une attaque et ne vient pas de l'IANA ou de l'AS112. Elle est entièrement de la faute des administrateurs de ces réseaux soi-disant attaqués. Un certain nombre de petits réseaux utilisent, soit parce qu'il n'y a plus d'adresses IPv4 disponibles <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, soit parce qu'ils croient à tort que cela leur apporte une certaine sécurité, des adresses IP privées, tirées du RFC 1918. Ces adresses étant spécifiques à un certain réseau, n'ayant pas de signification globale, les requêtes DNS demandant les noms associés à ces adresses ne devraient jamais sortir du réseau local (section 2 du RFC) et être toujours traitées par un serveur DNS interne. Mais, en pratique, c'est loin d'être le cas, et les serveurs de `in-addr.arpa`, le domaine utilisé pour la résolution d'adresses IP en noms (section 3), reçoivent un trafic important et inutile. Pour le traiter sans charger ces serveurs, les domaines servant aux plages d'adresses du RFC 1918 sont déléguées à l'AS112 (RFC 7534) qui est chargé de répondre « ce domaine n'existe pas » à toutes ces requêtes.

Mais, comme les requêtes de ce type sont des erreurs (rappelez-vous qu'elles n'auraient normalement jamais dû sortir), les réponses qu'envoie l'AS112 sont souvent inattendues pour le réseau local. Et, si le pare-feu ou l'IDS sont bizarrement configurés (ce qui est fréquent sur ces réseaux mal gérés), la

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7534.txt`

réponse DNS à leur question leur apparait comme une tentative d'attaque ! S'ils se plaignent, l'idée est de simplement leur renvoyer ce RFC 6305 à lire.

Ce RFC explique donc en termes simples ce que sont les adresses privées, ce qu'est la résolution d'adresses en noms, les raisons pour lesquelles est déployé l'AS112 (section 4 du RFC), et les noms et adresses des serveurs de l'AS112 (section 5) notamment le `prisoner.iana.org` qui donne son titre au RFC. Pour augmenter les chances que Google trouve cet article, je cite ici ces informations :

— `PRISONER.IANA.ORG` (`192.175.48.1`),
— `BLACKHOLE-1.IANA.ORG` (`192.175.48.6`),
— Et `BLACKHOLE-2.IANA.ORG` (`192.175.48.42`).

La section 6 explique ensuite le mécanisme par lequel la fausse alerte est déclenchée : un résolveur DNS du réseau local envoie la requête, par exemple `PTR 1.2.20.172.in-addr.arpa`, elle arrive aux serveurs de l'AS112, qui répondent, mais leurs réponses sont, pour des raisons diverses, bloquées. Normalement, le pare-feu ne couine pas pour chaque paquet bloqué mais, ici, les requêtes étant souvent déclenchées automatiquement par un logiciel, elles peuvent être nombreuses, provoquant de fréquentes réponses, qui peuvent ressembler à une attaque. Deux autres phénomènes expliquent cette perception : si la réponse est bloquée, la machine à l'origine de la requête va réessayer, souvent très vite. Et si le résolveur DNS refait ces essais avec des numéros de port croissant régulièrement, les réponses ressembleront à un balayage de ports.

Que devrait donc faire l'administrateur du site au lieu de harceler l'IANA ou les opérateurs de l'AS112 ? La section 7 lui donne quelques pistes, pour résoudre le problème qu'il a causé :

— Convaincre les machines terminales de ne pas chercher à résoudre les adresses en noms. Cela coupe le problème à la source, mais c'est évidemment assez difficile à faire dans un grand réseau, où l'administrateur du pare-feu ne contrôle pas forcément chaque machine. Par exemple, une bonne partie du trafic de l'AS112 provient des réseaux de téléphonie mobile et l'opérateur du pare-feu ne peut évidemment pas intervenir sur chaque téléphone.
— Bloquer sur le pare-feu non pas les réponses de l'AS112 mais les questions envoyées à ce service. Cela résoudrait complètement le problème de l'AS112 mais, sur le site, les résolutions des adresses en noms se bloqueraient, ce qui pourrait avoir des conséquences gênantes.
— Configurer les résolveurs du réseau local pour répondre avec autorité pour les zones correspondant aux adresses privées. C'est sans doute la solution la plus simple et le plus efficace à la fois. Elle est décrite avec plus de détails dans le RFC 6303.
— Plus "*geek*", mettre en place une instance locale de l'AS112 (RFC 7534).