PowerDNS permet de modifier facilement les réponses DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 juin 2008

https://www.bortzmeyer.org/powerdns-modifie-les-reponses-dns.html

---

Le serveur DNS récursif PowerDNS permet, depuis la version 3.1.7, de modifier facilement les réponses DNS, par exemple pour filtrer du contenu indésirable ou bien pour transformer les réponses « Domaine inexistant » en une réponse pointant vers un site Web d'aide. C'est, je crois, le premier récurseur à permettre cela, via une interface claire et bien documentée.

Il existe une forte demande de « réécriture » des réponses DNS. Par exemple, la justice peut imposer à un FAI de filtrer tel ou tel site illégal <http://www.zdnet.fr/actualites/internet/0,39020774,39381910,00.htm>. Ou bien un FAI peut vouloir mentir à ses clients en les dirigeant vers une page Web avec des publicités dès que ces clients font une faute de frappe et que le nom de domaine n'existe pas. Ces demandes étaient jusqu'à présent satisfaites en modifiant le source du résolveur (par exemple BIND), ou bien en programmant de zéro avec des bibliothèques comme Net : :DNS <http://www.net-dns.org/> en Perl.

Désormais, avec l'annonce de la version 3.1.7 <http://mailman.powerdns.com/pipermail/pdns-users/2008-June/005471.html> de PowerDNS, cette réécriture est démocratisée. Le serveur récursif PowerDNS appelle une fonction écrite en Lua avant de renvoyer la réponse et cette fonction peut modifier ladite réponse. Changer une valeur est désormais aussi simple que d'écrire un script Lua comme :

```
function nxdomain  ( ip, domain, qtype )
       if qtype ~= pdns.A then return -1, {} end  --  only A records
       if not string.find(domain, "^www%.") then return -1, {} end  -- only things that start with www.
       ret={}
       ret[1]={qtype=pdns.CNAME, content="www.example.com", ttl=3602}
       ret[2]={qname="www.example.com", qtype=pdns.A, content="192.0.2.4", ttl=3602}
       return 0, ret
end
```

Les notes de cette version parlent de l'utilité de ce service pour des « réécritures responsables ». Mais c'est là que le bât blesse. Certes, PowerDNS n'est qu'un outil, il n'est pas responsable des mauvaises utilisations qui ne manqueront pas d'être faites. Certes, il existe des utilisations légitimes d'un tel système (comme le filtrage des publicités <http://www.mvps.org/winhelp2002/hosts.htm> grâce au script en <http://www.fredan.org/nomoreads_pdns-recursor.tar>). Certes, si un serveur récursif est utilisé par une seule personne, elle a tout à fait le droit de modifier les réponses comme elle veut.

Mais la demande de réécriture des réponses DNS vient surtout de ceux qui veulent tromper leurs utilisateurs. Le cas le plus fréquent est celui de FAI peu scrupuleux qui renvoient, à la place du NXDOMAIN ("*No Such Domain*", nom non trouvé) l'adresse IP d'un de leurs serveurs Web, avec la publicité qui va avec.

Ces pratiques ont été critiquées dans le RFC 4924 [1], section 2.5.2. Mais il faudra plus qu'un RFC pour les faire cesser ! En attendant, il est dangereux de donner de tels outils à ceux qui n'hésitent pas à envoyer de fausses réponses à leurs propres clients.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4924.txt