

Il est recommandé de fermer les serveurs DNS récursifs ouverts

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 Mars 2006. Dernière mise à jour le 26 Janvier 2009

<http://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>

Suite, notamment, à une nouvelle attaque, il est sérieusement question en ce moment de créer une liste noire des serveurs DNS récursifs ouverts (i.e. qui acceptent et servent des requêtes récursives depuis tout l'Internet) et, peut-être, pour certains serveurs, par exemple de TLD, d'arrêter de répondre aux requêtes de ces serveurs DNS récursifs ouverts.

Bien qu'aucun consensus n'ait encore émergé et que, à ma connaissance, aucun "grand" domaine n'ait encore mis en œuvre ce refus de réponse, je crois prudent de prévenir les gérants de serveurs DNS : il est fortement conseillé de ne pas avoir de serveurs DNS récursifs ouverts. C'est aussi le conseil que donne le RFC 5358¹.

Notez que cette note ne mentionne que les risques que court l'Internet en raison de votre serveur. Votre serveur court aussi des risques, mais ils ne sont pas traités ici.

Vous pouvez voir si un serveur DNS est récursif avec la commande dig :

```
% dig @x.y.z.t SOA fr.  
...  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 9, ADDITIONAL: 13  
...
```

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5358.txt>

Et le "flag" "ra" dans la réponse indique que le serveur est récursif ("ra" veut dire "recursion available").

A priori, vos serveurs sont récursifs pour votre réseau local et c'est normal. Vous devez faire ce test depuis l'extérieur de votre réseau pour qu'il soit significatif. Si vous n'avez pas d'accès à une machine extérieure pour lancer dig, une bonne solution est l'interface Web de the Measurement Factory <<http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl>>.

Les détails techniques sur la meilleure façon d'arrêter de fournir un service DNS récursif ouvert sont exposés dans "Securing an Internet Name Server" <<http://www.cert.org/archive/pdf/dns.pdf>>. Si votre serveur de noms ne fait pas autorité, pour aucun domaine, le plus simple est d'en bloquer l'accès depuis l'extérieur, à la fois au niveau du coupe-feu (si le serveur a uniquement des adresses IP privées, c'est encore plus simple), et depuis les ACL du serveur.

La technique parfois citée d'utiliser `allow-recursion` avec BIND n'est pas du tout conseillée : cela n'interdit pas l'accès au cache du serveur DNS. Si l'attaquant réussit à peupler ce cache (par exemple en envoyant un courrier à une machine utilisant légitimement ce serveur récursif), il pourra quand même mener son attaque. BIND 9.4 a une nouvelle option `allow-query-cache` qui résoud ce problème. Avec cette option, une configuration raisonnable serait :

```
allow-recursion {mynetworks};
allow-query-cache {mynetworks}; // Surtout ne pas oublier celui-ci.
```

Une variante de l'attaque par réflexion et amplification, mais ne nécessitant pas que le récursif soit ouvert, est apparue en janvier 2009 <<http://www.bortzmeyer.org/dns-attaque-ns-point.html>>. Elle repose sur le fait que, même avec `recursion no`, certaines données hors-zone sont quand même distribuées au demandeur, par exemple la liste des serveurs de noms de la racine (d'où le requête NS . qu'on voit parfois dans le journal). Avec BIND, il vaut donc mieux avoir aussi `additional-from-cache no`.

Comme avec chaque mesure technique de protection, il existe des faux positifs : des usages légitimes vont se trouver gênés. Malheureusement, il n'existe pas de protection parfaite et sans défauts. On peut dire qu'il vaudrait mieux empêcher l'usurpation d'adresse IP, et donc mettre en œuvre les RFC 2827 et RFC 3704 mais cela semble irréaliste à court terme.

Parmi les raisons légitimes mentionnées, il y a le fait que certains FAI se permettent d'ajouter des réponses sur leurs serveurs de noms, par exemple en configurant des jokers, qui font que toute question aura une réponse, même lorsqu'elle n'aurait pas dû. À l'heure où j'écris, Noos fait hélas cela et Wanadoo l'a fait <<http://www.macadsl.com/actu/2006/01/27/detournement-de-traffic-chez-wanadoo-via-1>> (cela semble désormais arrêté). Voici ce que cela donne chez Noos (`list.debian.org` n'existe pas) :

```
$ host -v list.debian.org
...
;; ANSWER SECTION:
list.debian.org.      10000  IN      A       82.101.8.43
list.debian.org.      10000  IN      TXT     "NXDOMAIN"
```

<http://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>

Face à ces mauvaises pratiques, il est raisonnable d'installer sur le réseau un serveur de noms parlant directement à ceux de la racine **mais** il ne doit pas être récursif ouvert, pour les raisons citées ci-dessus.

Si on tient à ce que des usagers mobiles utilisent les serveurs de noms de leur réseau habituel, et non pas celui du point d'attachement actuel, la bonne solution n'est pas le serveur DNS récursif ouvert mais TSIG ou des techniques non-DNS comme le VPN ou IPsec.

J'ajoute que les serveurs faisant autorité devraient être séparés des serveurs récursifs, notamment pour éviter l'empoisonnement du cache des serveurs faisant autorité par les réponses aux requêtes. Le mieux est d'avoir deux machines (physiques ou virtuelles, par exemple avec Xen <http://www.bortzmeyer.org/xen.html>) séparées, mais on peut aussi avoir deux démons différents, sur deux adresses IP différentes, sur la même machine ou utiliser les vues de BIND 9, si on ne peut utiliser qu'une seule machine. Deux très bons tutoriels sur les vues sont http://www.oreillynet.com/pub/a/oreilly/networking/news/views_0501.html et http://www.howtoforge.com/two_in_one_dns_bind9_views.

Un peu de technique, maintenant. En quoi consiste cette attaque, exactement ? Une vieille attaque DoS utilisant le DNS est récemment devenue plus populaire grâce entre autre à des applications comme DNSSEC. Le principe (en très gros, et il y a des variantes) est le suivant : un attaquant A veut du mal à une victime V et il dispose de n relais R, sous forme de serveurs récursifs ouverts (à tous). Souvent, l'attaquant contrôle également un domaine D, servi par des serveurs faisant autorité, S.

A envoie une requête à R en imitant l'adresse de V (ce qui est trivial en UDP). La requête va arriver sur les serveurs S mais R va garder la réponse dans son cache. Et R va répondre à V, l'attaquant ainsi ("*It's like having a pizza delivered to a friend's house as a prank.*") décrit un bon article de vulgarisation http://redtape.msnbc.com/2006/03/the_real_threat.html). Si l'enregistrement est suffisamment gros, l'amplification peut être sensible (et s'accompagner d'effets rigolos dûs à la fragmentation). C'est là que DNSsec peut aider l'attaquant en augmentant l'amplification. A n'a pas grand'chose à faire.

Les serveurs de noms du TLD de S se sont limités à diriger R vers S.

D est vite repéré et supprimé par le domaine du dessus. Mais avec un gros TTL et le concours de R, l'attaque peut continuer longtemps après la suppression de D.

Une variante est celle où l'attaquant demande directement à S. S sera le seul réflecteur donc l'attaque est limitée par les capacités des deux ou trois serveurs de D. Alors qu'il y a des centaines de milliers de R.

Si D est un domaine innocent, l'attaque est moins pratique : il faut que D ait des enregistrements énormes (c'est là que DNSsec peut aider). Voici un exemple en utilisant un serveur récursif ouvert et tcpdump pour regarder la requête :

```
% dig +bufsize=2048 @192.0.2.233 ANY isc.org
...
;; MSG SIZE rcvd: 653

14:08:52.633001 > 0800 80: IP 213.41.181.9.33334 > 192.0.2.233.53: 39670+ [1au] ANY? isc.org. (36)
14:08:52.921382 < 0800 697: IP 192.0.2.233.53 > 213.41.181.9.33334: 39670 11/4/11 MX mx.sth1.isc.org. 15, [domain]
```

Le domaine `isc.org` a été choisi car il contient plusieurs gros enregistrements. On voit qu'on atteint $697 / 80 =$ un facteur 8,7 d'amplification. Sans même avoir besoin d'un domaine D à soi et sans DNSSEC...

Si D est coupable, tout est plus facile, son gérant met des enregistrements de type TXT de 8k et on a alors une énorme amplification.

Comme tout le système dépend de relais récursifs ouverts, la solution la plus couramment proposée est de créer une liste noire de ces relais, et que les serveurs du TLD refusent de leur répondre.

Il faut comparer ces futures listes aux listes de relais ouverts plutôt qu'aux listes d'émetteurs de spam ou bien aux listes d'adresse résidentielles. Car on peut déterminer objectivement et automatiquement si un serveur DNS est récursif ouvert.

L'avis de l'IETF est dans le RFC 5358. Pour la discussion sur la liste noire, voir <http://www.gossamer-threads.com/lists/nanog/users/89657>, <http://lists.oarci.net/pipermail/dns-operations/2006-February/thread.html>, http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf et <http://ccnog.org/archive/operations/msg00050.html>. Pour ceux qui s'inquiètent de la fermeture toujours plus grande d'Internet, je suis assez d'accord avec Andrew Sullivan <http://lists.oarci.net/pipermail/dns-operations/2006-March/000432.html> : le passé est passé, on peut le regretter mais pas au point d'être paralysé par lui. Pour un exemple d'attaque utilisant cette méthode, voir http://weblog.barnet.com.au/edwin/cat_networking.html. Une bonne analyse est <http://www.isotf.org/news/DNS-Amplification-Attacks.pdf>.