RFC 5358 : Preventing Use of Recursive Nameservers in Reflector Attacks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 octobre 2008

Date de publication du RFC : Octobre 2008

http://www.bortzmeyer.org/5358.html

L'ampleur des attaques DoS menées avec l'aide de serveurs DNS récursifs ouverts <http://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html> a mené à ce RFC qui résume les bonnes pratiques : un serveur DNS ne doit **pas** être récursif pour le monde entier.

L'accroissement du nombre d'attaques début 2006 a provoqué une prise de conscience, qui s'est manifesté par de nombreux avertissements aux administrateurs réseaux (comme celui de l'AFNIC <http://www.afnic.fr/actu/nouvelles/general/NN20060404>). La vitesse de publication d'un RFC étant ce qu'elle est, c'est seulement maintenant qu'un RFC met par écrit cette règle simple (le RFC est très court). Un serveur DNS ne doit être récursif que pour ses clients connus, pas pour tout l'Internet.

En effet, s'il est récursif ouvert, il peut servir de base à une attaque par amplification <http://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>. Il n'y a aujourd'hui aucune raison technique légitime de laisser un serveur récursif ouvert (vous pouvez tester le vôtre avec l'interface Web de the Measurement Factory <http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl> et trouver des informations sur la configuration de votre logiciel dans le document, malheureusement ancien, "*Securing an Internet Name Server*" <http://www.cert.org/archive/pdf/dns.pdf>).

La section 4 détaille les configurations qui peuvent limiter l'accès à la récursion : par exemple, pour un boîtier SOHO qui sert également de résolveur DNS, discriminer selon l'interface (n'accepter les requêtes DNS que si elles viennent du réseau local). Ou bien, pour les machines en déplacement (un des arguments les plus souvent présentés par ceux qui voulaient maintenir la récursion ouverte à tous), utiliser un résolveur local à la machine, ou bien monter un VPN avec un résolveur de confiance.

À noter que notre RFC parle également beaucoup de BCP 38 <http://www.bortzmeyer.org/bcp38.html> (actuellement le RFC 2827 [1]) comme étant la « vraie » solution au problème. Mais c'est exagéré : BCP 38 ne résoud pas tous les problèmes, notamment les attaques entres clients d'un même opérateur.

Une technique non mentionnée par le RFC est de limiter le trafic du résolveur <http://www.bortzmeyer.org/rate-limiting-dns-open-resolver.html>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt