RFC 8973 : DDoS Open Threat Signaling (DOTS) Agent Discovery

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 janvier 2021

Date de publication du RFC : Janvier 2021

https://www.bortzmeyer.org/8973.html

Le protocole DOTS, normalisé dans les RFC 8811[1], RFC 9132 et RFC 8783, sert à coordonner la réponse à une attaque par déni de service, entre la victime de l'attaque (le client DOTS) et un service d'atténuation de l'attaque (le serveur DOTS). Mais comment le client trouve-t-il son serveur ? Il peut y avoir une configuration manuelle, mais ce RFC propose aussi des moyens automatiques, basés sur un choix de plusieurs techniques, dont DHCP et NAPTR.

Attention, cela permet de trouver le serveur, mais pas le fournisseur du service d'atténuation. Car il faut un accord (souvent payant) avec ce fournisseur, et un échange de mécanismes d'authentification. Cette partie doit se faire manuellement. Le protocole de notre RFC prend ensuite le relais.

Notez aussi qu'il n'y a pas un seul moyen de découverte du serveur. La section 3 du RFC explique en effet que, vu la variété des cas d'utilisation de DOTS, on ne peut pas s'en tirer avec un seul mécanisme. Parfois le client a un CPE géré par le FAI, sur lequel on peut s'appuyer pour trouver le serveur DOTS, et parfois pas. Parfois, il faudra utiliser les résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html> d'un opérateur et parfois ce ne sera pas nécessaire. Parfois l'atténuateur est le FAI et parfois pas. Bref, il faut plusieurs solutions.

Voyons d'abord la procédure générale (section 4). Personnellement, je pense que le client DOTS doit donner la priorité aux configurations manuelles (DOTS est un système de sécurité, un strict contrôle de ce qui se passe est préférable). Mais le RFC ne décrit pas les choses ainsi. Il expose trois mécanismes, le premier, qualifié de configuration explicite, étant composé de deux techniques très différentes, la configuration manuelle ou bien DHCP. À noter au passage que la configuration manuelle peut indiquer le

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8811.txt

nom ou l'adresse IP mais, si elle indique l'adresse IP, le nom sera quand même obligatoire car il servira pour la vérification du certificat.

L'ordre des préférences entre ces mécanismes est imposé, pour que le résultat de la découverte soit prédictible. D'abord l'explicite (manuel ou DHCP, section 5), puis la résolution de service (section 6) puis la découverte de service (section 7).

Première technique automatique à utiliser, DHCP (section 5). Ce protocole va être utilisé pour récupérer le nom du serveur DOTS (le nom et pas seulement l'adresse IP car on en aura besoin pour authentifier la session TLS). Avec DHCPv6 (RFC 8415), l'option DHCP pour récupérer le nom est 141 <https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xml#dhcpv6-parameters-2> en IPv6 et 147 <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameter xml#options> pour IPv4. Une autre option permet de récupérer les adresses IP du serveur DOTS.

Deuxième technique, la résolution de service. Il faut partir d'un nom, qui peut être configuré manuellement ou bien obtenu par DHCP. Ce n'est pas le nom du serveur DOTS, contrairement au cas en DHCP pur, mais celui du domaine dans lequel le client DOTS se « trouve ». On va alors utiliser S-NAPTR (RFC 3958) sur ce nom, pour obtenir les noms des serveurs. L'étiquette à utiliser est `DOTS` pour le service (enregistré à l'IANA <https://www.iana.org/assignments/s-naptr-parameters/s-naptr-parameters.xml#s-naptr-parameters-1>) et `signal` (RFC 9132) ou `data` (RFC 8783) pour le protocole (également à l'IANA <https://www.iana.org/assignments/s-naptr-parameters/s-naptr-parameters.xml#s-naptr-parameters-2>). Par exemple si le client DOTS est dans le domaine `example.net`, il va faire une requête DNS de type NAPTR. Si le domaine comportait un enregistrement pour le service DOTS, il est choisi, et on continue le processus (compliqué !) de NAPTR ensuite. Si on cherche le serveur pour le protocole de signalisation, on pourrait avoir successivement quatre requêtes DNS :

```
example.net.   IN NAPTR 100 10 "" DOTS:signal.udp "" signal.example.net.

signal.example.net. IN NAPTR 100 10 "s" DOTS:signal.udp "" _dots-signal._udp.example.net.

_dots-signal._udp.example.net.  IN SRV   0 0 5000 a.example.net.

a.example.net.   IN AAAA  2001:db8::1
```

Troisième technique, la découverte de service (DNS-SD) du RFC 6763. On cherche alors un enregistrement de type PTR dans `_dots-signal.udp.example.net`. Il nous donnera un nom pour lequel on fera une requête SRV.

DOTS servant en cas d'attaque, il faut prévoir la possibilité que l'attaquant tente de perturber ou de détourner ce mécanisme de découverte du serveur. Par exemple, on sait que DHCP n'est pas spécialement sécurisé (euphémisme !). D'autre part, DOTS impose TLS, il faut donc un nom à vérifier dans le certificat (oui, on peut mettre des adresses IP dans les certificats mais c'est rare). Quant aux techniques reposant sur le DNS, le RFC conseille d'utiliser DNSSEC, ce qui semble la moindre des choses pour une technique de sécurité. Il suggère également de faire la résolution DNS via un canal sûr par exemple avec DoT (RFC 7858) ou DoH (RFC 8484).

Apparemment, il existe au moins une mise en œuvre de DOTS qui inclut les procédures de découverte de notre RFC, mais j'ignore laquelle.