RFC 8903 : Use cases for DDoS Open Threat Signaling

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 mai 2021

Date de publication du RFC : Mai 2021

https://www.bortzmeyer.org/8903.html

Le travail autour de DOTS ("*DDoS Open Threat Signaling*") vise à permettre la communication, pendant une attaque par déni de service, entre la victime et une organisation qui peut aider à atténuer l'attaque. Ce nouveau RFC décrit quelques scénarios d'utilisation de DOTS. Autrement, DOTS est normalisé dans les RFC 8811 [1] et ses copains.

Si vous voulez un rappel du paysage des attaque par déni de service, et du rôle de DOTS ("*DDoS Open Threat Signaling*") là-dedans, je vous recommande mon article sur le RFC 8612. Notre RFC 8903 ne fait que raconter les scénarios typiques qui motivent le projet DOTS.

Par exemple, pour commencer, un cas simple où le fournisseur d'accès Internet d'une organisation est également capable de fournir des solutions d'atténuation d'une attaque. Ce fournisseur (ITP dans le RFC, pour "*Internet Transit Provider*") est sur le chemin de tous les paquets IP qui vont vers l'organisation victime, y compris ceux de l'attaque. Et il a déjà une relation contractuelle avec l'utilisateur. Ce fournisseur est donc bien placé, techniquement et juridiquement, pour atténuer une éventuelle attaque. Il peut déclencher le système d'atténuation, soit à la demande de son client qui subit une attaque, soit au contraire contre son client si celui-ci semble une source (peut-être involontaire) d'attaque. (Le RFC appelle le système d'atténuation DMS pour "*DDoS Mitigation Service*" ; certains opérateurs ont des noms plus amusants pour le DMS comme OVH qui parle d'« aspirateur ».)

Dans le cas d'une demande du client, victime d'une attaque et qui souhaite l'atténuer, le scénario typique sera qu'une machine chez le client (un pare-feu perfectionné, par exemple), établira une session DOTS avec le serveur DOTS inclus dans le DMS du fournisseur d'accès. Lorsqu'une attaque est détectée (cela peut être automatique, avec un seuil pré-défini, ou bien manuel), la machine du client demandera l'atténuation. Pendant l'atténuation, le client pourra obtenir des informations de la part du DMS du

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

fournisseur. Si l'attaque se termine, le client pourra décider de demander l'arrêt de l'atténuation. Notez que la communication entre le client DOTS (chez la victime) et le serveur DOTS (chez le fournisseur d'accès) peut se faire sur le réseau « normal » (celui qui est attaqué) ou via un lien spécial, par exemple en 4G, ce qui sera plus cher et plus compliqué mais aura l'avantage de fonctionner même si l'attaque sature le lien normal.

Ce scénario simple peut aussi couvrir le cas du réseau domestique. On peut imaginer une "*box*" disposant de fonctions de détection d'attaques (peut-être en communiquant avec d'autres, comme le fait <https://project.turris.cz/en/security> la Turris Omnia) et d'un client DOTS, pouvant activer automatiquement l'atténuation en contactant le serveur DOTS du FAI.

Le second cas envisagé est celui où le fournisseur d'accès n'a pas de service d'atténuation mais où le client (mettons qu'il s'agisse d'un hébergeur Web), craignant une attaque, a souscrit un contrat avec un atténuateur spécialisé (de nombreuses organisations ont aujourd'hui ce genre de services, y compris sans but lucratif <https://deflect.ca/>). Dans ce cas, il faudra « détourner » le trafic vers cet atténuateur, avec des trucs DNS ou BGP, qui sont sans doute hors de portée de la petite ou moyenne organisation. L'accord avec l'atténuateur doit prévoir la technique à utiliser en cas d'attaque. Si c'est le DNS, la victime va changer ses enregistrements DNS pour pointer vers les adresses IP de l'atténuateur (attention au TTL). Si c'est BGP, ce sera à l'atténuateur de commencer à annoncer le préfixe du client (attention aux règles de sécurité BGP, pensez IRR et ROA), et au client d'arrêter son annonce. Le reste se passe comme dans le scénario précédent.