Utiliser les « middleboxes » de censure pour des attaques par déni de service

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 septembre 2021

https://www.bortzmeyer.org/middlebox-a-l-attaque.html

Une méthode courante pour réaliser une attaque par déni de service sur l'Internet est de trouver un **réflecteur**, une machine qui, sollicitée par l'attaquant, va envoyer des paquets vers la victime. Les bons (du point de vue de l'attaquant…) réflecteurs font en outre de l'**amplification**, émettant davantage de paquets et/ou d'octets qu'envoyés par l'attaquant. Un article <https://www.usenix.org/conference/usenixsecurity21/presentation/bock> à la conférence Usenix d'août 2021 expose un nouveau type de réflecteurs : les innombrables "*middleboxes*" placées pour censurer des communications sont tellement mal conçues qu'elles font d'excellents (du point de vue de l'attaquant…) réflecteurs.

Détaillons cet article, « "*Weaponizing Middleboxes for TCP Reflected Amplification*" <https://geneva.cs.umd.edu/papers/usenix-weaponizing-ddos.pdf> ». Le but d'un attaquant est de trouver de nombreux réflecteurs (plus ils sont nombreux, plus l'attaque sera efficace) mais aussi de maximiser l'amplification (on parle de BAF - "*Bandwidth Amplification Factor*" - pour le gain en octets et de PAF - "*Packet Amplification Factor*" - pour le gain en paquets). On a ainsi vu des attaques exploitant l'amplification de protocoles utilisant UDP, comme par exemple le DNS <https://www.bortzmeyer.org/amplification-dns-combien.html> ou bien NTP <https://www.bortzmeyer.org/ntp-reflexion.html>. Une des bases de l'attaque par réflexion étant de mentir <https://www.bortzmeyer.org/usurpation-adresse-ip.html> sur son adresse IP, a priori, ces attaques ne sont pas possibles avec TCP, qui protège contre cette usurpation (RFC 5961 [1]). Mais, en fait, on sait déjà que des attaques par réflexion avec TCP sont possibles <https://www.bortzmeyer.org/amplification-tcp.html>, et qu'elles ont parfois un bon BAF. C'est ce que développent les auteurs de l'article.

Comme réflecteurs, ils utilisent des "*middleboxes*", ces engins installés en intermédiaires sur un grand nombre de chemins sur l'Internet, qui examinent le trafic et agissent, souvent n'importe comment. Une utilisation courante des "*middleboxes*" est la censure, soit étatique (au niveau d'un pays), soit au niveau

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5961.txt

d'un réseau local. Par exemple, la "*middlebox*" va examiner le trafic HTTP et, si l'adresse IP de destination est sur sa liste de blocage, empêcher la communication. Une des façons de le faire est de prétendre être le vrai serveur et de renvoyer une page indiquant que la connexion est bloquée :

Arrivé là, vous commencez à voir comment cela peut être exploité pour une attaque : l'attaquant envoie un paquet TCP d'ouverture de connexion (paquet SYN) vers une adresse IP censurée, en usurpant l'adresse IP de la victime, et le message de censure, avec l'image, sera envoyée à la victime, fournissant un BAF sérieux.

Mais, là, vous allez me dire que ça ne marchera pas, TCP ne fonctionne pas comme cela : la "*middlebox*" n'arrivera pas à établir une session TCP complète puisque la victime ne répondra pas aux accusés de réception, ou bien enverra un paquet de fin de session (paquet RST). Mais c'est là que l'article devient intéresssant : les auteurs ont découvert que de nombreuses "*middleboxes*" ne font pas du TCP correct : elles envoient le message de censure (une page Web complète, avec images), sans attendre qu'une session TCP soit établie.

Ce n'est pas uniquement de l'incompétence de la part des auteurs des logiciels qui tournent dans la "*middlebox*". C'est aussi parce que, notamment dans le cas de la censure étatique, la "*middlebox*" ne voit pas forcément passer tous les paquets, le trafic Internet étant souvent asymétrique (si on a plusieurs liaisons avec l'extérieur). Et puis il faut aller vite et avoir le moins possible d'état à mémoriser. La "*middlebox*" ne se donne donc pas la peine de vérifier que la session TCP a été établie, elle crache ses données tout de suite, assomant la victime pour le compte de l'attaquant. L'amplification maximale observée (en octets, le BAF) a été de plus de 7 000...Et certains cas pathologiques permettaient de faire encore mieux.

Comment ont été trouvées les "*middleboxes*" utilisables ? Comme l'attaque ne marche que si la "*middlebox*" ne fait **pas** du TCP correct, les conditions exactes du déclenchement de la réflexion ne sont pas faciles à déterminer. Les auteurs ont donc envoyé une variété de paquets TCP (avec ou sans PSH, ACK, etc) et utilisé le système d'apprentissage Geneva <https://www.bortzmeyer.org/geneva.html> pour découvrir la solution la plus efficace. (Au passage, le meilleur déclencheur de la censure semble être `www.youporn.com`, largement bloqué un peu partout.) En balayant tout l'Internet avec ZMap, ils ont pu identifier un grand nombre de réflecteurs. Ils ne les ont évidemment pas utilisé pour une vraie attaque, mais des méchants auraient pu le faire, montrant ainsi le danger que présente ces boitiers bogués et largement répandus (ils sont très populaires auprès des décideurs), alors qu'ils fournissent une armée de réflecteurs prêts à l'emploi.

Certains réflecteurs arrivent même à des facteurs d'amplification incroyables, voire infinis (une fois un paquet envoyé par l'attaquant, le tir de barrage du réflecteur ne cesse jamais). Les auteurs expliquent cela par des boucles de routage, faisant passer le paquet déclencheur plusieurs fois par la "*middlebox*" (et parfois sans diminuer le TTL), ainsi que par des réactions aux réactions de la victime (qui envoie des paquets RST).

Des bons réflecteurs d'attaque ont été identifiés à des nombreux endroits, comme l'université Brigham Young ou la municipalité de Jacksonville. Identifier les produits utilisés a été plus difficile mais on pu repérer le Dell SonicWALL NSA 220 <https://www.amazon.com/SonicWALL-NSA-220-Firewall-Applia
dp/B0063REHE4> ou un équipement "*Fortinet*". D'un point de vue géopolitique, on notera que les réflecteurs sont situés un peu partout, avec évidemment davantage de présence dans les dictatures. Par contre, la Chine est assez peu représentée, leur système de censure étant (hélas) plus intelligement bâti.

---

https://www.bortzmeyer.org/middlebox-a-l-attaque.html