Un routeur de cœur de réseau peut-il espionner le trafic ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juin 2013

https://www.bortzmeyer.org/porte-derobee-routeur.html

Dans son médiatique rapport <https://www.bortzmeyer.org/rapport-bockel.html>, le sénateur Bockel affirmait que « Rien n'empêcherait, en effet, un pays producteur de ce type d'équipements [les routeurs de cœur de réseau] d'y placer un dispositif de surveillance, d'interception, [..] ». Est-ce réaliste ?

Si c'est possible, alors, comme la totalité des routeurs de cœur de réseau utilise du logiciel privateur sur lequel l'utilisateur n'a aucun contrôle, on peut en effet imaginer que le gentil routeur qu'on a installé nous trahit et envoit une copie de nos messages à Pékin (Bockel, qui est un nationaliste de mauvaise foi, ne cite que les routeurs Huawei comme si les Cisco, les Juniper ou même les Alcatel tricolores n'avaient pas exactement les mêmes possibilités. Cisco va jusqu'à les documenter publiquement <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/65LIch1.html>.) Un routeur étant un engin très complexe, une fonction supplémentaire dans son logiciel pourrait être difficile à voir.

Mais, franchement, je ne pense pas, pour des raisons de limites physiques, que ce soit réaliste. Il y a deux façons d'espionner le trafic : analyser sur le routeur et envoyer au maître espion une synthèse. Ou bien transmettre la totalité du trafic au maître qui pourra alors l'analyser.

Le premier nécessite des processeurs puissants puisqu'il faut analyser un trafic cumulé qui peut être de plusieurs Tb/s. Les routeurs typiques ont, curieusement (vu leur prix), des processeurs plutôt petits, l'essentiel du travail étant fait par des ASIC. On ne peut pas espérer faire une recherche de mots-clés avec ces processeurs. Il faudrait donc dissimuler dans le routeur des processeurs spécialisés, et espérer qu'ils ne seront jamais repérés. Or, les gens qui installent de tels routeurs les ouvrent souvent, ne serait-ce que pour installer de nouvelles cartes, et sont souvent curieux et compétents techniquement. Un tel dispositif matériel ne resterait sans doute pas longtemps secret (lisez un récit de découverte d'un tel dispositif <http://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf>). Et ce serait la fin des ambitions commerciales du constructeur qui serait ainsi attrapé la main dans le sac.

Notez que les fonctions d'espionnage pourraient en théorie être dans les ASIC, sur lesquels on n'a aucune information (même si tout le logiciel standard du routeur était libre). Cela affecterait toutefois leur taille et leur consommation électrique donc cela semble peu vraisemblable.

Enfin, l'arrivée de routeurs programmables (OpenFlow et autres SDN) introduit de nouvelles possibilités d'attaques : on pourrait reprogrammer le routeur pour lui faire écouter.

Je parlais ici d'une analyse complète du paquet, genre recherche plein texte, ou bien genre DPI. Mais on peut aller plus vite si on se contente d'analyser les métadonnées (comme les adresses IP de source et de destination). C'est moins riche mais, dans certains cas, cela peut être mieux que rien pour l'espion (analyse de trafic). Les routeurs savent déjà faire, avec leur matériel actuel, ce genre de travail, nécessaire pour les statistiques NetFlow (IPFIX aujourd'hui, cf. RFC 7011 [1]). Autre hypothèse, si on veut filtrer très vite le trafic, le routeur peut n'envoyer à l'espion que le trafic de/vers une adresse IP spécifique.

Dans tous les cas, une fois la synthèse faite, il faut l'envoyer au maître espion, ce qui peut être détecté (ce qui serait très gênant pour la firme qui fournit les routeurs). Une solution possible pour l'espion serait de ne pas transmettre directement les données mais indirectement, par exemple en faisant passer certains paquets envoyés par le maître et en en bloquant d'autres, selon la valeur des données qu'on veut faire sortir du routeur.

Bref, c'est peut-être possible mais avec des capacités d'espionnage plutôt limitées (officiellement, les dispositifs d'écoute légale ne sont pas prévus pour de l'écoute en masse). Est-ce de cela que parlait le rapport Bockel ? Pour les consultants en cyberpeur, cela serait certainement moins efficace de ne parler que de surveillance ciblée.

Bon, si analyser un tel trafic total en temps réel sur le routeur n'est pas possible, peut-on le transmettre en vrac afin de l'analyser tranquillement dans des centres de données où le maître espion aurait tous les moyens matériels nécessaires ? Là, on se heurte aux limites de la physique. Si un routeur a quinze interfaces à 10 Gb/s (c'est petit, pour un routeur de cœur, songez aussi que les interfaces à 100 Gb/s commencent à apparaître), il faudrait pouvoir faire passer 150 Gb/s de trafic vers Pékin ! Non seulement c'est physiquement impossible avec les interfaces réseau dont dispose le routeur, mais cela se remarquerait (tous les opérateurs regardent leur données NetFlow, c'est le cœur de leur métier).

Enfin, notons aussi que les routeurs de cœur sont chers et viennent souvent avec une offre de maintenance, voire un technicien à demeure. L'humain a certainement des possibilités d'espionnage plus élevées que le routeur...

Surtout, ce qu'oublie de dire le rapport Bockel (mais ce n'est pas un oubli : son vrai but est le protectionnisme, pas la sécurité) est que le vrai espionnage ne se fait pas par des astuces techniques sophistiquées sur les routeurs. Il se fait surtout aux extrémités, où le trafic est facilement écoutable (et pas uniquement par les Chinois, cf. PRISM, une attaque extrêmement "*low-tech*").

Ceci dit, dans tous les cas, il est prudent, lorsqu'on fait une analyse de sécurité, de supposer que le trafic est écouté (après tout, mon analyse peut avoir des failles, ne basez pas votre sécurité uniquement sur cet article). Si ce n'est par le routeur, cela peut être par d'autres biais <http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> (on trouve même des SFP qui savent espionner <http://www.jdsu.com/ProductLiterature/PacketPortal-difference-be pdf>). Et, donc, pensez à chiffrer tout votre trafic. C'est le B. A. BA de la confidentialité, que ce soit contre l'APL ou contre d'autres espions. Attention, cela ne protège que le voyage, la sécurité des extrémités est une autre question.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7011.txt

Dans un article récent d'Andréa Fradin <http://www.slate.fr/story/71673/peut-on-casser-internet>, un autre risque est discuté, celui où une porte dérobée dans le routeur permettrait l'arrêt soudain de celui-ci, faisant ainsi une attaque par déni de service. Ce point est également mentionné dans le rapport Bockel (« voire un système permettant d'interrompre à tout moment l'ensemble des flux de communication »). Là, on ne peut rien dire. Une telle porte dérobée est techniquement possible quoique non triviale (les routeurs de cœur sont en général configurés de manière à ne pas recevoir de trafic de l'extérieur ; il faudrait donc que l'ordre vienne dans un des paquets qui transite par le routeur). Elle serait difficile à détecter puisque, comme indiqué plus haut, le logiciel des routeurs n'est pas du logiciel libre (notez que le rapport Bockel, tout occupé à voir des Chinois partout, ne mentionne pas du tout cette possibilité évidente d'améliorer la sécurité).

Il est rigolo de se dire que, compte tenu du nombre de bogues accidentelles dans les routeurs (un routeur, cela ressemble à une grosse boîte bruyante, mais en fait c'est plein de logiciel), une telle porte dérobée pourrait facilement passer pour une bogue. Cela permettrait au fabricant de nier toute action malveillante. Moins drôle, comme des mécanismes d'espionnage existent déjà dans les routeurs (cf. la documentation de Cisco citée plus haut), on pourrait imaginer un espion qui, sans avoir besoin d'instrumenter le routeur lui-même, se contente d'exploiter une fonction d'espionnage existante (celles-ci ne sont pas forcément bien protégées).

Notez qu'une telle porte dérobée pourrait être utilisée pour bien d'autres choses que d'arrêter le routeur brutalement. Elle pourrait permettre par exemple de détourner ou de jeter une partie du trafic, par exemple en tripotant les tables de routage.

Vous pouvez aussi lire un article de Wired sur le piratage des routeurs par la NSA <http://www.wired.com/threatlevel/2013/09/nsa-router-hacking/>.

Merci à Olivier Laurelli, Ollivier Robert et Jean-Baptiste Favre pour les intéressantes discussions sur « comment, lorsqu'on est Empire du Mal, mettre une porte dérobée dans un routeur ». Merci à Frédéric Gander, Emmanuel Thierry, Alex Archambault, Thomas Mangin, Julien Rabier, Alexandre Dulaunoy, Phil Regnauld et Jérôme Nicolle pour d'utiles critiques et ajouts à cet article. À noter que j'ai eu aussi des messages privés de gens travaillant pour des fabricants de routeurs ou des opérateurs de télécommunications ne souhaitant pas que leur nom soit publié. Donc, merci aux anonymes.