La faille de sécurité BGP de 2008

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 août 2008

https://www.bortzmeyer.org/faille-bgp-2008.html

Des failles de sécurité sur Internet, il y en a. Des failles concernant le protocole de routage BGP, il y en a. Que dire de particulier sur celle annoncé à Defcon en août 2008 ?

Notons d'abord la mise en scène. Comme le disait un participant de Nanog : « *"I think they saw the DNS people getting their 10 minutes of fame and wanted their own"* :) ». La sécurité informatique est un métier, comme le show-business : il faut faire parler de soi. Ce n'est pas par hasard que les exposés à Defcon commencent toujours par « cette faille est particulièrement sérieuse ». On n'a jamais vu un chercheur en sécurité débuter avec « C'est une petite vulnérabilité sans intérêt. ». Prendre conscience de cela aide à mettre cette annonce dans son contexte.

Ensuite, la faille de sécurité en question est-elle réellement nouvelle ? Non et oui. Non, car elle ne contient que des éléments déjà bien connus comme les limites du modèle de sécurité de BGP (BGP est normalisé dans le RFC 4271 [1] et le RFC 4274 fournit une bonne analyse du protocole), qui avait par exemple été bien illustrées par l'attaque de Pakistan Telecom contre YouTube <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>. Oui parce qu'une combinaison intelligente de techniques connues est en soi une nouveauté. Ce qu'ont présenté Anton Kapela & Alex Pilosov à Defcon est une réelle percée.

En quoi consiste t-elle ? Le socle sur lequel elle s'appuie est le fait que n'importe quel routeur BGP de la planète (donc, en pratique, n'importe quel opérateur, ou craqueur ayant piraté un opérateur), peut annoncer la route qu'il veut et elle se propagera, dans certaines conditions, à tous les autres routeurs BGP du monde, faisant ainsi converger le trafic vers les routeurs choisis par l'attaquant. Par exemple, si je veux récupérer le trafic de Paypal, j'observe que leur annonce BGP est pour le préfixe 66.211.160.0/19, j'annonce 66.211.168.0/24 (un préfixe plus spécifique, pour être sûr qu'il se propage et qu'il soit utilisé, tout en couvrant quand même les adresses IP de www.paypal.fr) et hop, je récupère les paquets destinés à Paypal.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4271.txt

Mais, évidemment, ça se voit : la grande ouverture de l'Internet, qui fait sa vulnérabilité, est aussi sa principale ligne de défense, la base de son système immunitaire. N'importe qui peut utiliser un "*looking glass*" et voir qui est l'attaquant. Il y a même des services d'alerte automatique <https://www.bortzmeyer.org/alarmes-as.html> bâtis sur ce principe (commme MyASN <http://www.ris.ripe.net/myasn.html> ou bien Renesys Route Intelligence <http://www.renesys.com/products_services/routing_intelligence/>). Et, surtout, tout le trafic étant dévié, le service normal s'arrête et tout le monde peut faire un traceroute pour voir à cause de qui. Grâce à cela, l'attaque de Pakistan Telecom avait tourné court.

La première innovation de Kapela & Pilosov était donc de bloquer les méthodes de détection les plus simples en acheminant le trafic détourné vers son destinataire légitime. Si l'attaquant ne veut pas réaliser une DoS mais simplement espionner le trafic, cela lui permet d'être plus discret (cela porte le doux nom, emprunté à l'électricité, de "*BGP shunt*"). Cela ne stoppe pas les alarmes des systèmes comme MyASN mais cela empêche la détection immédiate. Il est probable que la majorité des sites qui sont ainsi attaqués ne se rendent compte de rien (tout le monde n'est pas abonné à MyASN).

La redirection est délicate à réussir : il faut que tout l'Internet achemine le trafic de la victime vers l'attaquant **sauf** les réseaux qui sont sur le chemin de retour choisi, de façon à ce que le trafic puisse revenir à son destinataire légitime. Kapela & Pilosov utilise pour cela l'"*AS prepending*" en mettant dans le chemin d'AS de l'annonce BGP des valeurs qui assureront le rejet de la route de retour pour tous... sauf pour les routeurs du chemin de retour que les attaquants ont choisi.

La deuxième innovation de nos deux chercheurs est de modifier le TTL dans les paquets IP qu'ils voient passer, pour rendre encore plus difficile la détection par la victime.

Faut-il s'inquiéter ? Oui. Même s'il n'y a rien de révolutionnaire dans cette attaque, on peut dire qu'elle démocratise le détournement BGP, comme l'attaque Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html> démocratisait les empoisonnements de caches DNS.

Que peut-on faire ? D'abord, le site normal, qui n'est pas opérateur. Il ne peut pas faire grand'chose pour empêcher le "*shunt*" mais il peut se protéger en utilisant systématiquement des mécanismes de sécurisation de bout en bout, notamment la cryptographie (par exemple SSH et jamais telnet). Ainsi, même détourné, le trafic révèlera nettement moins de chose. Mais c'est essentiellement aux opérateurs d'agir. Si on a son propre numéro d'AS, il est recommandé de s'inscrire aux mécanismes d'alarme cités plus haut. Si on est opérateur ou auteur de logiciel BGP, on peut vérifier ses règles de filtrage, se demander s'il ne serait pas une bonné idée d'utiliser un IRR (sans se faire d'illusions : la qualité des données qu'on y trouve est loin d'être parfaite) ou espérer le déploiement de technologies de sécurisation de BGP comme RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>, "*Secure BGP*" <http://www.ir.bbn.com/sbgp/> et soBGP <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html> (celles-ci ont du mal à décoller, non pas qu'elles soient trop compliquées mais parce qu'elles ont en commun de nécessiter la création d'une nouvelle infrastructure de confiance, avec ce que cela suppose de problèmes organisationnels et politiques. Le RFC 5123 en explique certains.)

L'article qui a fait le plus de bruit est " *Revealed : The Internet's Biggest Security Hole*" <http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html>. C'est un article très sensationnaliste, une de ses plus grosses erreurs est de reprendre le discours standard : "*Those protocols were largely developed in the 1970s with the assumption that every node on the then-nascent network would be trustworthy.*" En fait, les concepteurs de l'Internet à l'époque (au fait, BGP est bien plus récent que « les années 70 ») étaient bien conscients de ces problèmes mais, même si on repartait de zéro, on ne pourrait pas les résoudre facilement (il n'existe pas d'État policier mondial qui pourrait attribuer des « licences

d'opérateur » et des certificats X.509 afférents pour pouvoir signer les annonces BGP). Le second article de Wired, "*More on BGP Attacks – Updated*" <http://blog.wired.com/27bstroke6/2008/08/how-to-intercep.html> est bien meilleur, surtout pour les détails techniques. Mais le mieux est de lire les transparents originaux <http://blog.wired.com/27bstroke6/files/edited-iphd-2.ppt> des deux découvreurs de la faille (également sur le site de Defcon <http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf>).

Sur BGP, on peut aussi lire mon cours pratique <https://www.bortzmeyer.org/deux-cours-routage.html>.