# BGP et DNS : attaques sur les protocoles critiques de l'Internet

Nicolas Dubée

Secway/BD Consultants
ndubee@secway.fr

## 1 Introduction

Le 11 septembre 2001 n'aura fait que renforcer un constat de nombreux gouvernements : une nation est tributaire d'un certain nombres d'infrastructures critiques telles que les pôles énergétiques, les moyens de communication et d'information nécessaires à la continuité économique et administrative du pays. Aux Etats-Unis, Internet a été jugé critique dès 1996 par l'administration Clinton. Une commission d'experts fut alors mandatée pour évaluer menaces et risques pesants sur la Toile. Deux acronymes sont revenus régulièrement tout au long des nombreux rapports en résultant : DNS et BGP. Ainsi, le groupe de hackers L0PHT déclarait-il en 1998 devant le Sénat américain pouvoir semer le chaos sur Internet en moins de 30 minutes, sans doute en référence à l'un de ces deux protocoles. Si DNS est maintenant maîtrisé en terme de connaissance des risques et contre-mesures, BGP relève encore du domaine mystique des protocoles au cœur d'Internet. Nous tâcherons donc dans cette présentation d'éclairer le lecteur quant au fonctionnement et aux vulnérabilités connues du protocole BGP. Nous en déduirons les risques liés à BGP et les pistes de sécurisation actuelles.

## 2 Aperçu de BGP

Une des caractéristiques les plus innovantes des protocoles Internet a été l'arrivée du routage dynamique et complètement logique du trafic. Les acteurs clefs de ce concept sont les routeurs : véritables équipements réseaux destinés à aiguiller des paquets, les routeurs disposent de tables internes leur indiquant par où envoyer le paquet pour qu'il arrive au bon destinataire. Si cette tâche d'aiguillage est simple sur de petites topologies (on préconfigure le routeur pour envoyer le paquet où on souhaite), elle devient complexe dès lors que les routes peuvent changer en fonction de la vie du réseau : c'est le cas par exemple de réseaux connectés à d'autres par plusieurs chemins. On a donc introduit des protocoles permettant de reconfigurer automatiquement les tables de routage en fonction d'évènements tels que la perte de connexion sur une route ou l'équilibrage du trafic entre plusieurs routes.

Ces protocoles sont appelés IGP (*Interior Gateway Protocol*) lorsqu'ils fonctionnent sur des réseaux internes, ou EGP (*Exterior Gateway Protocol*) autrement. Les protocoles communément trouvés sont RIP, OSPF, ... Cependant, la

topologie d'Internet a atteint une complexité telle qu'un protocole de routage aussi simple que RIP était impossible à utiliser. En effet, la cascade de chemins mais surtout de responsabilités administratives était telle qu'il a été décidé de regrouper les réseaux non plus d'après leur préfixe (c'est-à-dire d'après leur adresse réseau, combinaison adresse IP+masque de réseau), mais en groupes de préfixes sous la même autorité appelés AS : Autonomous Systems identifiés par des numéros. Par exemple, un prestataire d'accès Internet dispose de son propre AS regroupant son réseau ainsi que les réseaux de ses petits clients. Chaque AS a alors la charge de dire au monde entier quels réseaux il héberge afin que les autres sachent par où accéder à ces réseaux.

Le protocole BGP fut conçu dans ce but, annoncer les réseaux et échanger les informations de routage entre AS. Pour ce faire, des sessions sont établies entre les routeurs externes d'un AS et ceux de ses voisins. Ces routeurs (appelés pairs ou peers) dialoguent par échange de messages au format BGP, dont le fonctionnement exact est décrit dans le RFC 1771 (la forme utilisée actuellement étant la version 4 depuis 1994-1995). Ces sessions BGP sont en fait de simples connexions TCP établies de manière permanente par un routeur vers le port 179 de l'autre et sur laquelle sont échangés 4 types de messages : Open, Update, Notify, Keepalive.

Alors qu'Open, notify et keepalive ne sont pas à proprement parler porteurs d'information de routage, le message Update sert à véhiculer les nouvelles annonces ou les préfixes à retirer.

En BGP, toute annonce porte sur un préfixe : on annonce au reste du monde l'arrivée sur Internet du réseau 12.34.56.0/24 par exemple. Le message est alors propagé après vérification aux pairs du pair, chaque AS traversé y ajoutant son propre numéro. Un chemin d'AS est construit avec la progression du message sur Internet : chaque annonce qui arrive sur un pair contient la liste des AS à traverser pour arriver au préfixe annoncé. Une table de routage globale est ainsi construite grâce au seul protocole BGP.

A l'heure actuelle, on estime qu'environ 120000 préfixes Internet sont annoncés par ces mécanismes. Aucune alternative n'est facilement possible puisqu'elle nécessiterait de revoir tout le mécanisme d'annonces, constitué uniquement autour de BGP.

## 3 Vulnérabilités

On comprend donc bien que BGP est critique pour le fonctionnement d'Internet. On peut d'ailleurs à ce propos citer quelques incidents comme l'incident AS7007 en 1997 (du numéro de l'AS d'où provenait l'incident) qui a résulté sur une panne globale d'Internet pendant 2 heures. Cette panne était liée uniquement à une mauvaise configuration d'un routeur chez un hébergeur Internet en Floride, le mécanisme de distribution BGP entraînant une diffusion de l'erreur. En terme de vulnérabilités sécuritaires, les problèmes du protocole BGP sont nombreux et bien connus. On distingue en général les grands points suivants :

- Authentification : pas d'authentification requise entre les pairs. Même s'il est possible de configurer son routeur pour s'authentifier auprès de ses pairs, ceci est purement optionnel et de toute façon insuffisant puisque le canal TCP en lui-même n'est pas sécurisé.
- Autorisation : pas de mécanisme simple pour la vérification de la pertinence des informations trouvées dans les messages. Un routeur peut par exemple annoncer le préfixe qu'il souhaite, même un ne lui appartenant pas. Le pair recevant cette annonce n'a aucun moyen simple de faire la vérification, surtout s'il se trouve au cœur d'Internet, loin de la source de l'annonce.

Ces deux grandes classes de vulnérabilités sont amplifiées par le fait que comme vu précédemment, BGP ne dispose d'aucune vérification et sécurisation cryptographique du flux TCP : il est dès lors possible d'intercepter, modifier, insérer, rejouer, un flux BGP pour exploiter les deux grandes classes précédentes.

## 4 Risques associés

Quels sont les risques associés à ces vulnérabilités ? Les risques de déni de service sont évidemment les plus importants, mais on peut aussi imaginer l'altération de routes vers des serveurs ou réseaux sensibles dans un but de piratage (captation des flux notamment,...) Nous allons maintenant étudier les différents risques sous-jacents aux vulnérabilités exposées précédemment :

- Déni de service direct sur le routeur : tout routeur BGP peut être la cible d'un déni de service classique tel que le SYN flood. Le routeur est alors soit complètement planté, soit très lent. Dans ce cas, il ne peut indiquer en temps voulu à son pair qu'il est toujours en vie (message Keepalive). Dans ce cas, le pair considère que le routeur est planté, et purge les routes associées. Une nouvelle session est alors négociée par un des pairs, et l'attaque peut recommencer. La faisabilité d'une telle attaque est haute si le routeur n'est pas particulièrement protégé ou dimensionné, notamment au niveau de sa file d'attente des connexions en cours de négociation.
- Réinitialisation (RST) de la session BGP entre deux pairs : la session BGP étant transportée sur un flux TCP classique, on peut envisager la réinitialisation de cette connexion par envoi (spoof) de paquets RST savamment choisi. Il en résulte alors comme précédemment la purge des routes associées au pair, puis la tentative de redémarrage d'une session. Cependant, en terme de faisabilité, cette attaque nécessite la connaissance de nombreux paramètres : l'adresse IP des deux pairs, le port source de la connexion TCP, la fenêtre des numéros de séquence, et le TTL à 1 (ce qui peut être obtenu en voyant combien de hops on traverse avant d'arriver au routeur cible). Cette attaque est donc très délicate à réaliser mais théoriquement possible en aveugle, sans accès au réseau des pairs. Les paragraphes suivants montreront que même si l'attaque RST décrite ici est perçue comme simple à réaliser, elle est en fait très délicate à mettre en œuvre et bien moins préoccupante que d'autres.

- Spoofing complet de sessions : on crée en aveugle de toutes pièces une session de peering BGP avec une victime, vers laquelle on peut injecter des routes, en enlever,... En pratique, on se retrouve dans la même situation de faisabilité que l'attaque précédente, avec en plus la nécessité d'avoir le numéro de séquence TCP exact et tous les attributs BGP requis par le peer qu'on essaie de flouer. Cette attaque relève donc de la gageure, sachant qu'il faut en plus paralyser temporairement le peer qu'on essaie de spoofer.
- Hijacking de sessions existantes : variation de l'attaque précédente, mais au lieu de créer complètement une session, on réutilise une session existant entre deux peers dans laquelle on injecte des paquets de type update ou notify. Les paramètres à déterminer sont les mêmes que précédemment, même s'il ne suffit là que d'un paquet, la négociation TCP ayant déjà été faite par les peers officiels. On voit donc bien que les attaques en aveugle sont très difficiles à réaliser, en raison notamment du fait que BGP fait dialoguer entre eux des pairs préconfigurés : l'administrateur a préalablement réglé dans chaque routeur l'adresse du peer distant. L'attaque d'un point de vue technique se résume donc à un spoof TCP classique, maintenant très difficile à faire. On peut cependant imaginer que ces attaques soient réalisables si le réseau des pairs est écouté par le pirate. Dans ce cas, il lui vaudrait bien mieux attendre que l'administrateur se connecte à l'un des routeurs, la plupart du temps en telnet !

  Les attaques suivantes nécessitent d'avoir accès à un routeur BGP officiel. Elles ne sont donc plus aveugles comme précédemment, mais sont beaucoup plus facilement réalisables. Il convient en effet de se souvenir que BGP est un protocole massivement distribué, où les pairs ne s'authentifient et ne s'autorisent que très faiblement. Le pirate peut donc compromettre un routeur BGP situé chez un hébergeur faible, pour l'utiliser afin d'envoyer de fausses annonces. Voyons les effets possibles de telles annonces.
- Désagrégation : en BGP, les préfixes plus spécifiques (c'est à dire plus longs) sont prioritaires. Ainsi, une annonce pour un réseau /24 à l'intérieur d'un /16 prendra précédence sur l'annonce du /16, et seule l'annonce /24 sera gardée pour le préfixe correspondant. Un agresseur peut donc complètement désagréger un grand réseau en envoyant des annonces pour des parties de ce grand réseau. Ces annonces plus spécifiques vont être prises en compte et le réseau va être complètement partitionné en fonction des annonces faites. Le risque associé est principalement un déni de service, mais on peut imaginer qu'un agresseur extraie d'un réseau important une petite plage contenant des serveurs sensibles, qu'il fait renvoyer chez lui (voir attaques suivantes). Notons à propos de la désagrégation l'expérience AS7007 en avril 1997 où un modeste prestataire en Floride a désagrégé pratiquement l'ensemble d'Internet, rendant le réseau des réseaux inopérant pendant deux heures et fortement perturbé pendant la journée.
- Injection de routes : les préfixes annoncés n'étant pas systématiquement vérifiés par le pair, il est possible d'annoncer à son pair un préfixe pour

lequel on n'a pas autorité. Couplé avec le principe de priorité des préfixes vu précédemment, un agresseur peut annoncer le préfixe contenant sa victime. Tout le trafic venant de la zone touchée par l'annonce et destiné à la victime sera routé vers l'agresseur, qui aura tout loisir sur la suite : abandon complet (donc déni de service), Man-in-the-Middle avec manipulation des données avant réexpédition vers la victime, masquerade du serveur sensible, ... D'autre part, une attaque indirecte est possible : pourquoi ne pas annoncer par exemple le préfixe de plusieurs des root-servers DNS ? L'injection de route peut être moins ciblée et porter sur des blocs normalement d'utilisation bien spécifique comme les DUSA (blocs réservés tels que 192.168.0.0/16) ou même les blocs non alloués, entraînant une saturation des tables BGP sur les routeurs touchés et même des perturbations sur les réseaux utilisant un adressage Interne.

Le point le plus critique des attaques précédentes est qu'elles peuvent justement ne pas être des attaques ! En effet, la plupart des incidents répertoriés actuellement sur BGP sont des erreurs de configuration résultant sur l'injection de routes erronées ou la propagation d'annonces de réseaux privés. Notons finalement qu'il est justifié de s'interroger sur l'homogénéité du parc des core routers Internet. Une faute d'implémentation de la stack BGP sur ces matériels pourrait mettre à terre bon nombre d'entre eux, étant donné le peu de diversité du parc en terme de constructeurs différents. Un constat similaire a été fait début 2003 sur l'homogénéité logicielle des root-servers DNS : tous étaient équipés du logiciel BIND. Il a été décidé de passer un des root-servers sur NSD, concurrent de BIND ne partageant aucun code avec ce dernier.

## 5 Conclusion et recommandations

Les risques liés à BGP sont donc autant des attaques que des erreurs de configuration. Les enjeux sont la survie de blocs entiers du réseau Internet, mais même si le danger peut sembler énorme, la compétence globale des personnels aux échelons sensibles liés à BGP et les mesures prises actuellement sur la majorité des équipements devraient permettre de limiter l'impact de telles attaques.

Les alternatives à BGP sont pour l'instant trop complexes à déployer, et toutes les infrastructures nécessaires ne sont de toute façon pas disponibles. Citons cependant la piste la plus sérieuse pour le futur de BGP : Secure-BGP (S-BGP), actuellement en phase de maturation technologique. S-BGP authentifie les peers et sécurise le flux par un canal IPsec. D'autre part, chaque annonce est autorisée par un mécanisme de certification type PKI, dont les autorités pressenties sont les organismes de gestion des blocs d'adresses : ARIN, APNIC, RIPE, ... Quelques projets concurrents tels que SOBGP sont en lice mais il est difficile de dire si l'un d'entre eux peut faire face à S-BGP.

S-BGP n'étant pas encore utilisable en situation réelle, la sécurisation de BGP se résume à l'application des fameuses BCP (Best Common Practices) :

- forcer l'authentification MD5 des peers - filtrer les annonces venant de ses clients, pour vérifier qu'ils annoncent bien les préfixes leur ayant été assignés
- filtrer les annonces sortant de chez soit, pour vérifier que seules les classes possédées sont attribuées
- filtrer les annonces venant d'autres AS, pour vérifier si possible qu'elles correspondent bien aux peers, et sinon qu'elles ne contiennent pas de classes DUSA ou de blocs non assignés.
- protéger ses routeurs
- ne pas avoir de route par défaut
- faire le peering sur une interface secondaire ou sur un loopback.