

Groupe de travail Réseau
Request for Comments : 3882
 Catégorie : Information
 Traduction Claude Brière de L'Isle

D. Turk, Bell Canada

septembre 2004

Configurer BGP pour bloquer les attaques de déni de service

Statut de ce mémoire

Le présent mémoire apporte des informations à la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2004).

Résumé

Le présent document décrit une technique de fonctionnement qui utilise les communautés BGP pour déclencher à distance la transformation en trou noir d'un réseau de destination particulier pour bloquer des attaques de déni de service. La mise en trou noir peut être appliquée sur un choix de routeurs plutôt qu'à tous les routeurs parlant BGP dans le réseau. Le document décrit aussi une technique de tunnel d'évacuation qui utilise les communautés et les tunnels BGP pour tirer le trafic dans un routeur d'évacuation pour analyse.

Table des Matières

| | |
|--|---|
| 1. Techniques existantes de trou noir déclenché par BGP..... | 1 |
| 2. Technique améliorée de trou noir déclenché par BGP..... | 2 |
| 3. Tunnels d'évacuation..... | 3 |
| 4. Considérations sur la sécurité..... | 4 |
| 5. Remerciements..... | 4 |
| 6. Référence pour information..... | 4 |
| 7. Adresse de l'auteur..... | 4 |
| 8. Déclaration complète de droits de reproduction..... | 4 |

1. Techniques existantes de trou noir déclenché par BGP

Les techniques actuelles de trou noir déclenché par BGP s'appuient sur l'altération de l'adresse de prochain bond BGP d'un réseau ciblé par une attaque à travers les réseaux iBGP. Une annonce iBGP personnalisée est générée à partir d'un routeur qui participe au système autonome de destination/attaqué où l'adresse de prochain bond pour le réseau ou hôte ciblé est modifiée pour pointer sur une adresse de réseau privé de la [RFC1918]. La plupart des routeurs de l'Internet, en particulier les routeurs de bordure, ont des chemins statiques qui pointent sur des adresses de la RFC1918 vers l'interface nulle. Ces chemins statiques dirigent tout le trafic destiné au réseau attaqué sur l'interface nulle.

Lorsque un routeur à capacité iBGP à l'intérieur du système autonome de destination reçoit la mise à jour de iBGP, le préfixe annoncé va être ajouté au tableau d'acheminement avec un prochain bond de un des réseaux mentionnés dans la RFC1918. Le routeur va alors tenter de résoudre le prochain bond RFC1918 afin de qualifier le chemin et déduire une interface de transmission. Ce processus va retourner un prochain bond valide vers l'interface nulle. En supposant que le routeur est configuré de façon appropriée pour diriger le trafic destiné à un réseau privé de la RFC1918 sur une interface nulle, le trafic destiné au réseau attaqué sera éliminé, rendant le réseau attaqué injoignable pour l'attaquant ou pour tous les autres.

Bien que cette technique protège l'infrastructure interne de l'attaque, en protégeant un grand nombre d'appareils, elle a le désagréable effet collatéral de rendre le réseau ciblé/attaqué injoignable à travers le système autonome tout entier. Même si un chemin statique qui pointe sur une adresse de la RFC1918 vers une interface nulle n'est pas configuré sur tous les routeurs au sein du système autonome de destination, la modification du prochain bond rend le trafic non acheminable à sa destination légitime.

Les opérateurs de réseau utilisent habituellement les trous noirs déclenchés par BGP pendant une brève période. La technique cause des abandons de trafic sur tous les points d'entrée du système autonome pour le trafic destiné au réseau attaqué. Par défaut, les routeurs qui éliminent le trafic dans une interface nulle devraient envoyer un message "ICMP injoignable" à l'adresse de source appartenant au système autonome d'origine/attaquant.

Une fois que la procédure atteint ce point, une des adresses de source du trafic d'attaque est capturée par l'introduction d'un appareil avec la même adresse IP de source dans le domaine BGP du système autonome de destination/attaqué. L'appareil qui capture l'adresse de source collecte les paquets ICMP injoignable. Les adresses de source de ces paquets ICMP injoignable révèlent de quels routeurs bordure au sein du système autonome de destination/attaqué vient l'attaque. L'opérateur du réseau peut alors choisir d'arrêter manuellement le trafic sur les routeurs par lesquels entre le trafic de l'attaque.

2. Technique améliorée de trou noir déclenché par BGP

Le présent document décrit une technique développée pour donner pour instruction à un ensemble choisi de routeurs d'altérer l'adresse du prochain bond d'un préfixe particulier par l'utilisation du protocole BGP. Le prochain bond peut soit être une interface nulle, soit, comme on l'explique plus loin dans le présent article, une interface de tunnel d'évacuation.

Cette technique n'implique pas de liste d'accès ni de déclaration de limitation de débit pour traiter le trafic d'attaque, ni n'implique de changement à l'échelle du réseau de l'adresse de prochain bond du préfixe attaqué. Le prochain bond va seulement être changé sur une sélection de routeurs avec l'aide des communautés BGP au sein du système autonome de destination/attaqué.

Pour préparer le réseau à cette technique, l'opérateur a besoin de définir une valeur unique de communauté pour chaque routeur bordure du système autonome de destination qui pourrait conduire le trafic d'attaque à la victime. Par exemple, un réseau avec un numéro de système autonome BGP de 65001 a deux routeurs bordure (R1 et R2). La valeur de communauté de 65001:1 est allouée pour identifier R1, la valeur de communauté de 65001:2 est allouée pour identifier R2, et la valeur de communauté de 65001:666 est allouée pour identifier à la fois R1 et R2.

Après l'allocation de la communauté BGP, R1 et R2 doivent être configurés avec ce qui suit :

1. Un chemin statique qui pointe sur un réseau de la RFC1918 vers une interface nulle.
2. Une liste d'accès de chemins de système autonome qui correspond à l'annonce de préfixe BGP local.
3. Une liste d'accès de communauté BGP qui correspond à la valeur de communauté allouée par l'opérateur du réseau pour le routeur concerné (c'est-à-dire, 65001:1 pour R1).
4. Une liste d'accès de communauté BGP qui correspond à la valeur de communauté allouée par l'opérateur du réseau pour tous les routeurs (c'est-à-dire, 65001:666 pour R1 et R2)
5. Dans le traitement BGP, une politique iBGP d'importation de chemin devrait être appliquée sur les annonces iBGP reçues pour appliquer la logique suivante (les déclarations sont dans un ordre ET logique) :
 - a. Une déclaration de politique pour permettre les chemins qui satisfont aux critères suivants et appliquent les changements suivants :
 - i. satisfaire à une communauté spécifique de ce routeur (c'est-à-dire, 65001:1, pour R1) ;
 - ii. satisfaire au chemin d'AS des annonces BGP générées en local ;
 - iii. régler le prochain bond BGP à un réseau de la RFC1918 ;
 - iv. écraser la communauté BGP par la communauté bien connue (pas-d'annonce).
 - b. Une déclaration de politique pour permettre les chemins qui satisfont les critères suivants et appliquent les changements suivants :
 - i. satisfaire à une communauté qui couvre tous les routeurs (c'est-à-dire, 65001:666) ;
 - ii. satisfaire au chemin de système autonome pour les annonces BGP générées en local ;
 - iii. régler le prochain bond BGP à un réseau de la RFC1918 ;
 - iv. écraser la communauté BGP par la communauté bien connue (pas-d'annonce).

Après que les politiques ont été configurées sur R1 et R2, l'opérateur du réseau peut, dans le cas d'une attaque, annoncer le réseau ciblé qui pourrait être un ou plusieurs chemins "d'hôte" /32 dans iBGP du système autonome de destination/attaqué. L'annonce doit contenir la valeur de communauté associée au ou aux routeurs où l'attaque arrive en plus de la communauté bien connue (no-export). L'utilisation des communautés BGP préserve l'adresse originale de prochain bond du réseau ciblé sur tous les routeurs où la configuration de la politique de chemin spécial n'est pas présente. iBGP va alors porter l'annonce de préfixe à tous les routeurs dans le système autonome de destination/attaqué. Tous les routeurs au sein du système autonome de destination, sauf ceux qui satisfont à la communauté marquée par le préfixe, vont oublier la valeur de communauté et vont installer le chemin de réseau avec l'adresse de prochain bond légitime. Les routeurs qui correspondent à la communauté vont aussi installer le chemin de réseau dans leur tableau d'acheminement mais vont altérer l'adresse de prochain bond en une adresse de réseau RFC1918 et ensuite en une interface nulle conformément à la configuration des politiques d'acheminement et

de recherche de chemin récurrent. La raison de la confrontation aux réseaux annoncés en local est de s'assurer qu'aucun homologue eBGP ne puisse faire un mauvais usage de cette communauté pour conduire un réseau à une interface nulle. La mise en trou noir des hôtes ciblés/attaqués est recommandée, mais pas le bloc d'adresses entier auquel ils appartiennent afin que l'effet du trou noir ait l'impact minimum sur le réseau attaqué.

Cette technique arrête la transmission du trafic à sa destination légitime sur les routeurs identifiés comme routeurs de transit du trafic d'attaque et qui ont des correspondances de carte d'acheminement pour la valeur de communauté associée à l'annonce de réseau. Tout autre trafic sur le réseau va continuer d'être transmis à la destination légitime, minimisant donc l'impact sur le réseau ciblé.

3. Tunnels d'évacuation

À la suite de la "technique améliorée de trou noir déclenché par BGP", il peut devenir nécessaire de regarder le trafic d'attaque pour mieux l'analyser. Cette exigence ajoute à la complexité de l'exercice. Habituellement, avec les interfaces de diffusion, les opérateurs de réseau installent des renifleurs sur un accès étendu d'un commutateur pour l'analyse du trafic. Une autre méthode serait d'annoncer un préfixe de réseau qui couvre l'adresse de l'hôte d'attaque dans iBGP, en altérant le prochain bond dans un appareil d'évacuation qui puisse enregistrer le trafic aux fins d'analyse. La première technique a pour résultat de mettre par terre les services offerts sur les adresses IP ciblées/attaquées. Le trafic inter-AS va être aspiré dans l'évacuation, avec le trafic intra-AS. L'analyse au niveau du paquet implique de rediriger le trafic hors de l'hôte de destination sur un renifleur ou un routeur. Par suite, si le trafic à examiner inclut du trafic légitime, celui-ci ne va jamais arriver à l'hôte de destination. Il en résulte un déni de service pour le trafic légitime.

Une meilleure alternative serait d'utiliser un tunnel d'évacuation. Un tunnel d'évacuation est mis en œuvre à tous les points d'entrée possibles à partir desquels des attaques peuvent passer dans le système autonome de destination/attaqué. En utilisant la technique de la communauté BGP, le trafic destiné à l'hôte attaqué/ciblé pourra être dérouté sur un chemin spécial (tunnel) où un renifleur pourra capturer le trafic et l'analyser. Après analyse, le trafic va sortir du tunnel et être acheminé normalement à l'hôte de destination. En d'autres termes, le trafic va passer du réseau à un renifleur sans altérer les informations de prochain bond du réseau de destination. Tous les routeurs au sein du domaine iBGP du système autonome de destination/attaqué vont avoir l'adresse de prochain bond appropriée. Seul le routeur de point d'entrée va avoir ses informations de prochain bond qui sont altérées.

Pour rentrer dans le détail de la procédure, un routeur d'évacuation avec un renifleur facultatif attaché à son interface est installé et configuré à participer à l'IGP et l'iBGP du système autonome attaqué. Ensuite, un tunnel est créé, en utilisant l'ingénierie de trafic MPLS comme exemple, à partir de tous les routeurs bordure d'où des attaques peuvent éventuellement provenir (trafic inter-AS) vers le routeur d'évacuation. Lorsque un hôte ou un réseau est attaqué, une annonce iBGP personnalisée est envoyée pour annoncer l'adresse réseau du ou des hôtes attaqués avec le prochain bond approprié qui assure que le trafic va atteindre ces hôtes ou réseaux. L'annonce personnalisée va aussi avoir une valeur de chaîne de communauté qui correspond à l'ensemble des routeurs bordure d'où entre l'attaque, comme décrit à la section 2. La nouvelle adresse de prochain bond configurée au sein de la section de politique d'acheminement de tous les routeurs bordure devrait être l'adresse IP de l'évacuation. Cette adresse IP appartient au sous réseau /30 alloué au tunnel qui connecte le routeur bordure au routeur d'évacuation.

Les routeurs qui ne correspondent pas à la chaîne de communauté vont faire l'acheminement régulier. Le défaut de correspondance à la chaîne de communauté sur ces routeurs va assurer que la politique de chemin spécial ne change pas l'adresse du prochain bond. Le trafic qui entre depuis les routeurs bordure et qui ne correspond pas à la communauté spéciale va passer à travers les interfaces régulières du routeur vers sa destination légitime. Il peut aussi être nécessaire de permettre au trafic d'atteindre sa destination après avoir été capturé. Dans ce cas, un chemin de réseau par défaut est configuré pour pointer sur toute interface rattachée et configurée sur le réseau iBGP. Cela inclurait aussi la même interface physique sur laquelle est bâti le tunnel. Comme l'adresse de prochain bond n'est pas changée sur l'appareil d'évacuation, le trafic qui entre dans cet appareil à partir du tunnel sera renvoyé au réseau du fait de la présence du chemin par défaut. Les protocoles d'acheminement prendront alors soin de l'acheminement approprié du trafic à sa destination d'origine (le réseau attaqué).

Il devient évident que cette technique peut aussi être utilisée pour des besoins autres que l'analyse du trafic de l'attaque. Le trafic légitime pourrait aussi être tiré hors de son acheminement normal dans un tunnel et ensuite réinséré dans le cœur de réseau sans altérer le schéma d'adressage du prochain bond à travers le réseau iBGP.

L'ingénierie du trafic MPLS, avec ses nombreux dispositifs, est une bonne méthode pour faire glisser du trafic vers l'appareil d'évacuation. Des dispositifs comme les politiques de qualité de service peuvent être appliqués au trafic d'attaque, l'empêchant ainsi d'entrer en compétition avec le trafic légitime.

Pour être capable d'altérer le prochain bond sur le routeur bordure, un sous réseau d'un réseau de la RFC1918 est acheminé

statiqument sur l'interface du tunnel. Un exemple de chemin statique est : ip route 192.168.0.12 255.255.255.255 Tunnel0

Régler le prochain bond de l'adresse IP cible à 192.168.0.12/32 va forcer le trafic à passer à travers le tunnel.

Le trafic est reçu à l'interface d'évacuation via le tunnel TE. Ensuite, trois méthodes peuvent être installées, à savoir des politiques de limitation de débit, des politiques de qualité de service, et des listes d'accès. Ces politiques peuvent limiter le débit ou éliminer le trafic classé comme trafic d'attaque. Ce processus sera achevé sur l'interface de l'appareil d'évacuation. Une autre application utile pour un routeur d'évacuation est de tirer le trafic via des tunnels jusqu'à une interface d'entrée et d'avoir une déclaration de chemin par défaut qui transmette le trafic sur une interface Ethernet. L'interface Ethernet est connectée au réseau iBGP et garantit cependant une livraison appropriée du trafic, elle permet quand même l'utilisation d'un renifleur de paquet pour mieux analyser le trafic d'attaque.

Ceci devient très utile lorsque il n'est pas faisable d'appliquer une liste d'accès ou une déclaration de limitation de débit sur le routeur BGP de bordure ou sur le routeur de dernier bond avant l'hôte ou le réseau attaqué parce que le matériel ou le logiciel ont des limitations. Donc, au lieu de renforcer les interfaces au point d'entrée du trafic d'attaque, ce dernier pourrait être tiré dans l'évacuation et traité sur cet appareil. Les coûts de fonctionnement peuvent être minimisés si le routeur d'évacuation est un appareil puissant.

4. Considérations sur la sécurité

Il est très important d'exercer un étroit contrôle sur les points d'échange eBGP avant de mettre en œuvre les techniques décrites dans le présent mémoire. Les clients eBGP peuvent être capables de transformer en trou noir un sous réseau particulier en utilisant les communautés Trou Noir. Pour éliminer le risque, la confrontation des annonces BGP générées en local dans la politique d'acheminement spéciale ne devrait pas être négligée.

5. Remerciements

L'auteur du présent document tient à remercier les développeurs de la technique du trou noir déclenché à distance et les développeurs de la technique de rétro dispersion pour collecter le trafic rétro dispersé. L'auteur remercie aussi tous les membres du département d'ingénierie IP de leur aide pour la vérification de la fonctionnalité de cette technique.

6. Référence pour information

[RFC1918] Y. Rekhter et autres, "Allocation d'[adresse pour les internets privés](#)", BCP 5, février 1996.

7. Adresse de l'auteur

Doughan Turk
Bell Canada
100 Wynford Drive

mél : doughan.turk@bell.ca

8. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.