Normes de sécurité d'acheminement convenues d'un commun accord (MANRS)

Introduction

La sécurité, en général, est un domaine difficile lorsqu'il s'agit d'incitations. La sécurité de l'infrastructure mondiale de l'internet, qu'il s'agisse du DNS ou du routage, pose des problèmes supplémentaires : l'utilité des mesures de sécurité dépend des actions coordonnées de nombreuses autres parties.

Tout au long de l'histoire de l'internet, la collaboration entre les participants et la responsabilité partagée de son bon fonctionnement ont été deux des piliers qui ont soutenu la croissance et le succès considérables de l'internet, ainsi que sa sécurité et sa résilience. Les solutions technologiques sont ici un élément essentiel, mais la technologie seule ne suffit pas. Pour stimuler des améliorations visibles dans ce domaine, un changement plus important vers la culture de la responsabilité collective est nécessaire.

Ce document vise à capturer cet esprit de collaboration et à fournir des orientations aux opérateurs de réseau pour traiter les questions de sécurité et de résilience du système mondial de routage Internet. Un autre objectif important est de documenter l'engagement des leaders de l'industrie à aborder ces questions, ce qui devrait amplifier l'impact à mesure que de nouveaux partisans se joignent à eux.

Objectifs

1. Sensibiliser et encourager les actions en démontrant l'engagement du groupe croissant de supporters
2. Promouvoir la culture de la responsabilité collective pour la résilience et la sécurité du système de routage mondial de l'internet
3. Démontrer la capacité de l'industrie à traiter les questions de résilience et de sécurité du système de routage mondial de l'internet dans un esprit de responsabilité collective
4. Fournir un cadre permettant aux FAI de mieux comprendre et d'aider à résoudre les problèmes liés à la résilience et à la sécurité du système de routage mondial de l'internet

Champ d'application

Il existe de nombreuses recommandations différentes pour améliorer la sécurité et la résilience du système de routage inter-domaines. Certains conseils peuvent même sembler quelque peu contradictoires et souvent la décision clé peut se résumer à comprendre ce qui est le plus important ou le plus approprié pour un réseau donné compte tenu de sa taille et de ses ressources, du nombre de connexions externes, de clients et d'utilisateurs finaux dont il dispose, de la taille et de l'expertise de son personnel, etc.

Les actions attendues et avancées ci-dessous soulignent un ensemble de recommandations qui sont certainement précieuses pour la sécurité et la résilience globales du système de routage mondial, ainsi que pour l'opérateur de réseau lui-même. Elles portent sur trois grandes catégories de problèmes :

- Problèmes liés à des informations d'acheminement incorrectes ;
- les problèmes liés au trafic avec des adresses IP source usurpées ; et
- Problèmes liés à la coordination et à la collaboration entre les opérateurs de réseau.

Les actions attendues définissent un "paquet" minimum - un ensemble de recommandations qui devraient certainement être mises en œuvre par les opérateurs qui soutiennent ce document MANRS. Ce paquet n'est pas exhaustif et l'on s'attend à ce que de nombreux opérateurs de réseau mettent déjà en œuvre des mesures et des contrôles encore plus stricts, ou prévoient de le faire à l'avenir. Les actions avancées présentées plus loin dans ce document élargissent encore le paquet minimum.

Nous sommes conscients du fait qu'une action particulière ne constitue pas une solution globale aux problèmes décrits. Mais chacune est un petit pas qui, s'il est multiplié par un grand nombre de partisans, peut devenir une amélioration significative de la résilience du système mondial de routage Internet. C'est pourquoi la sélection des actions a été basée sur une évaluation de l'équilibre entre les coûts individuels marginaux et faibles et le bénéfice commun potentiel.

Définitions

Afin d'articuler les spécificités des actions attendues et avancées, il est nécessaire de définir explicitement un certain nombre de termes, en rapport avec leur usage général dans l'industrie de l'internet.

- Infrastructure - Réseaux internes de l'opérateur, qui doivent être accessibles sur l'internet.
- Utilisateur final - Réseaux au sein du domaine de routage et d'administration d'un opérateur.
- Réseau de pairs - Réseau externe avec lequel est échangé le trafic relatif à vos infrastructures respectives et aux réseaux de clients.
- Réseau de transit - Réseau externe vers lequel le trafic relatif à votre infrastructure et à vos réseaux de clients est envoyé, mais à partir duquel le trafic de l'internet en général est reçu.
- Réseau de clients - Réseau externe pour lequel un opérateur fournit des services de transit.
- Single Homed K Un lien unique et simple entre les réseaux, ou la connexion d'un utilisateur final à l'infrastructure. Il s'agit d'un chemin unique sur lequel le trafic peut circuler à l'intérieur des réseaux ou entre eux.
- Multi Homed K Chemins multiples entre les réseaux (même les réseaux multiples), ou connexions entre un utilisateur final et l'infrastructure ; cela peut créer des chemins multiples sur l'infrastructure et l'Internet sur lesquels le trafic peut circuler.

Principes

1. L'organisation (ISP/opérateur de réseau) reconnaît la nature interdépendante du système de routage mondial et son propre rôle dans la contribution à un Internet sûr et résilient.
2. L'organisation intègre les meilleures pratiques actuelles en matière de sécurité et de résilience du routage dans ses processus de gestion de réseau, conformément aux actions.
3. L'organisation s'engage à prévenir, détecter et atténuer les incidents de routage grâce à la collaboration et à la coordination avec les pairs et les autres fournisseurs d'accès Internet, conformément aux actions.
4. L'organisation encourage ses clients et ses pairs à adopter ces principes et actions.

Actions attendues

1. Empêcher la propagation d'informations de routage incorrectes.

- L'opérateur de réseau définit une politique de routage claire et met en œuvre un système qui garantit l'exactitude de ses propres annonces et des annonces de ses clients vers les réseaux adjacents avec préfixe et granularité ASKpath.
- Les opérateurs de réseau peuvent communiquer à leurs réseaux adjacents les annonces qui sont correctes.
- L'opérateur de réseau fait preuve de diligence raisonnable lorsqu'il vérifie l'exactitude des annonces de ses clients, en particulier le fait que le client détient légitimement l'ASN et l'espace adresse qu'il annonce.

2. Empêchez le trafic avec des adresses IP source usurpées.

- L'opérateur de réseau met en œuvre un système qui permet la validation de l'adresse source pour au moins les réseaux de clients de type "singleKhomed stub", leurs propres utilisateurs finaux et leur infrastructure. L'opérateur de réseau met en œuvre un filtrage antiK spoofing pour empêcher les paquets ayant une adresse IP source incorrecte d'entrer et de sortir du réseau.

3. Faciliter la communication et la coordination opérationnelles globales entre les opérateurs de réseau.

- L'opérateur de réseau maintient des coordonnées de contact mises à jour et accessibles dans le monde entier.

Actions avancées

- 4. Faciliter la validation des informations de routage à l'échelle mondiale.
- L'opérateur de réseau a une politique de routage, des ASN et des préfixes publiquement documentés qui sont destinés à être annoncés à des parties externes.

Elaboration et références

Action 1. Empêcher la propagation d'informations de routage incorrectes.

- L'opérateur de réseau définit une politique de routage claire et met en œuvre un système qui garantit l'exactitude de ses propres annonces et des annonces de ses clients vers les réseaux adjacents avec préfixe et granularité du chemin AS.
- Les opérateurs de réseau peuvent communiquer à leurs réseaux adjacents les annonces qui sont correctes.
- L'opérateur de réseau fait preuve de diligence raisonnable lorsqu'il vérifie l'exactitude des annonces de ses clients, en particulier le fait que le client détient légitimement l'ASN et l'espace adresse qu'il annonce.

Discussion : Le plus important est de sécuriser les publicités de routage entrantes, en particulier en provenance des réseaux des clients, par l'utilisation de filtres *explicites au* niveau des préfixes ou de mécanismes équivalents. En second lieu, les filtres de chemin AS peuvent être utilisés pour exiger que le réseau du client soit explicite quant aux systèmes autonomes (AS) qui se trouvent en aval de ce client. D'autre part, les filtres de cheminement AS qui bloquent les annonces des clients de systèmes autonomes avec lesquels le fournisseur a une relation sans règlement peuvent empêcher certains types de "fuites" de routage. Le filtrage des annonces BGP des clients par les seuls filtres AS-path est *insuffisant* pour prévenir des problèmes de routage catastrophiques au niveau systémique.

Références :

"Recommended Internet Service Provider Security Services and Procedures", section Infrastructure de réseau, http://www.rfcKeditor.org/bcp/bcp46.txt

"BGP operations and security", http://tools.ietf.org/html/draftKietfKopsecKbgpKsecurity

Border Gateway Protocol Security, NIST : Publication spéciale SP 800K54, http://csrc.nist.gov/publications/nistpubs/800K54/SP800K54.pdf

"Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", http://tools.ietf.org/html/rfc3871

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

"Using the RIPE Database as an Internet Routing Registry", https://labs.ripe.net/Members/denis/usingKtheKripeKdatabaseKasKanKinternetKroutageKregistry

BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Action 2. Empêcher le trafic avec des adresses IP source usurpées.

- L'opérateur de réseau met en œuvre un système qui permet la validation de l'adresse source pour au moins les réseaux de clients à domicile unique, leurs propres utilisateurs finaux et leur infrastructure. L'opérateur de réseau met en œuvre un filtrage antispoofing pour empêcher les paquets ayant une adresse IP source incorrecte d'entrer et de sortir du réseau.
- Discussion : Des approches communes à ce problème ont impliqué des fonctionnalités logicielles telles que la SAV (Source-Address Validation) sur les réseaux de modems câble ou la validation stricte de l'uRPF (unicast Reverse-Path Forwarding) sur les réseaux de routeurs. Ces méthodes peuvent alléger la charge administrative dans les cas où le routage et la topologie sont moins relativement dynamiques. Une autre approche pourrait consister à utiliser les informations de filtrage des préfixes entrants pour créer un filtre de paquets, qui n'autoriserait que les paquets ayant des adresses IP sources pour lesquelles le réseau pourrait légitimement faire de la publicité sur l'accessibilité.

Références :

"Network Ingress Filtering" : Defeating Denial of Service Attacks which employ IP Source Address Spoofing", http://tools.ietf.org/html/bcp38

"Ingress Filtering for Multihomed Networks", http://tools.ietf.org/html/bcp84

"Securing the Edge", http://www.icann.org/committees/security/sac004.txt

"RIPE AntiKSpoofing Task Force HOWKTO", http://www.ripe.net/ripe/docs/ripeK 431

BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Action 3. Faciliter la communication et la coordination opérationnelles globales entre les opérateurs de réseau.

- L'opérateur de réseau maintient des coordonnées de contact mises à jour et accessibles dans le monde entier.

Discussion : Les lieux communs pour maintenir de telles informations sont PeeringDB, les bases de données whois des RIR et les grands IRR comme RADB et RIPE. Un opérateur de réseau doit enregistrer et maintenir des informations de contact 24 heures sur 24 et 7 jours sur 7 dans au moins une de ces bases de données. Ces informations de contact doivent inclure les coordonnées actuelles du point de contact de l'opérateur pour le NOC de l'AS, tous les netblocks et les noms de domaine. Les opérateurs sont encouragés à documenter leurs politiques de routage de réseau dans un IRR. Des informations supplémentaires sont également les bienvenues, comme par exemple une URL en miroir dans le champ approprié de leur enregistrement PeeringDB.

Références :

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

Peering DB, https://www.peeringdb.com RADB,

http://www.radb.net/

Action 4. Faciliter la validation des informations de routage à l'échelle mondiale.

- L'opérateur de réseau a une politique de routage, des ASN et des préfixes publiquement documentés qui sont destinés à être annoncés à des parties externes.

Discussion : Pour faciliter la validation des informations de routage par d'autres réseaux à l'échelle mondiale, il est nécessaire de disposer d'informations sur la politique de routage, les ASN et les préfixes qui sont destinés à être annoncés aux parties externes.

L'un des moyens de rendre la politique accessible au public consiste à les documenter à l'aide de RPSL dans l'un des registres de routage Internet (IRR) reflétés par la RADB (par exemple RIPE, ARIN, RADB, etc.). Dans ce cas, les opérateurs doivent enregistrer et maintenir au moins un (ou plusieurs) objet IRR "as-set" contenant une liste d'ASN destinés à être annoncés à des parties externes, qui pourraient être utilisés par des outils automatiques pour générer des filtres de préfixes. Les opérateurs doivent également maintenir leurs informations dans l'IRR pour s'assurer qu'elles sont à jour.

Un autre moyen plus sûr de faciliter la validation à l'échelle mondiale est le système RPKI. Les opérateurs pourraient obtenir des certificats RPKI pour leurs propres préfixes auprès des RIR qui leur ont attribué ces préfixes, et publier et maintenir des ROA correspondant aux préfixes qu'ils annoncent.

Les opérateurs doivent encourager leurs opérateurs de réseaux de clients à faire de même. Cela permettra aux autres réseaux de valider les annonces à l'échelle mondiale.

Références :

" L'utilisation de la RPSL en pratique

",http://tools.ietf.org/html/rfc2650 "

“Utilisation de la base de données RIPE comme registre de

routage Internet ",
https://labs.ripe.net/Members/denis/usingKtheKripeKdatabaseKasKanKinternetKroutingKregistry

"Opération de validation de l'origine basée sur l'infrastructure à clé publique de ressources (RPKI)", http://www.rfcKeditor.org/bcp/bcp185.txt