Groupe de travail Réseau J. Damas, ISC
Request for Comments : 5358 F. Neves, Registro.br
BCP 140
Catégorie : Bonnes pratiques actuelles
Traduction Claude Brière de L'Isle octobre 2008

Empêcher l'utilisation de serveurs de noms récurrents dans les attaques par réflexion

Statut du présent mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit les moyens d'empêcher l'utilisation des serveurs de noms récurrents configurés par défaut comme réflecteurs dans les attaques de déni de service (DoS). Il fournit des recommandations de configuration comme mesures pour atténuer l'attaque.

Table des matières

1. Introduction

Récemment, le DNS [RFC1034] a été désigné comme un facteur majeur de la génération d'une quantité massive de trafic réseau utilisé dans des attaques de déni de service (DoS). Ces attaques, appelées des attaques de réflecteur, ne sont pas dues à une faute particulière de la conception du DNS ni de ses mises en œuvre, mais au fait que le DNS s'appuie fortement sur UDP, dont l'abus facile est à la source du problème. Les attaques ont utilisé de façon préférentielle le DNS du fait de ses configurations par défaut courantes qui permettent une utilisation facile des serveurs de noms ouverts courants qui utilisent une telle configuration par défaut.

De plus, du fait du petit potentiel de grandes réponses d'interrogation du système DNS, il est facile de donner une grande amplification au trafic de source comme trafic réfléchi sur les victimes.

Les serveurs d'autorité du DNS qui ne fournissent pas de récurrence aux clients peuvent aussi être utilisés comme des amplificateurs ; cependant, le potentiel d'amplification est largement réduit quand des serveurs d'autorité sont utilisés. Il est aussi impraticable de restreindre l'accès aux serveurs d'autorité à un sous ensemble de l'Internet, car leur fonctionnement normal s'appuie sur leur capacité de servir une large audience ; donc, les opportunités d'atténuer l'échelle d'une attaque en modifiant les configurations de serveurs d'autorité sont limitées. Les recommandations du présent document visent seulement les serveurs de noms récurrents.

Dans le présent document on décrit les caractéristiques de l'attaque et on recommande des configurations de serveur DNS qui atténuent spécifiquement le problème décrit, tout en pointant sur la seule solution réelle : le déploiement à grande échelle du filtrage d'entrée pour empêcher l'utilisation d'adresses IP usurpées [RFC2827].

2. Terminologie du document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Description du problème

Parce que la majeure partie du trafic du DNS est sans état par conception, un attaquant peut commencer une attaque de DoS de la façon suivante :

1. L'attaquant commence par configurer un enregistrement dans une zone quelconque à laquelle il a accès, normalement avec une grande RDATA et une longue durée de vie (TTL, *Time to Live*).

2. Tirant parti de clients sur des réseaux non conformes à la [RFC2827] (BCP38) l'attaquant construit ensuite une interrogation en utilisant l'adresse de source de la victime cible et l'envoie à un serveur de noms récurrent ouvert.

3. Chaque serveur de noms récurrent ouvert procède à la résolution, met l'enregistrement en antémémoire, et finalement l'envoie à la cible. Après cette première recherche, l'accès aux serveurs de noms d'autorité n'est normalement plus nécessaire. L'enregistrement va rester en antémémoire au serveur de noms récurrent ouvert pour la durée du TTL, même si il est supprimé de la zone.

4. Nettoyer la zone pourrait, selon la mise en œuvre utilisée dans le serveur de noms récurrent ouvert, donner un moyen de nettoyer l'enregistrement en antémémoire du serveur de noms récurrent ouvert. Cela pourrait éventuellement impliquer des interrogations qui leurrent le serveur de noms récurrent ouvert et l'amènent à chercher des informations pour le même nom que celui utilisé dans l'amplification.

Parce que les caractéristiques de l'attaque impliquent normalement un faible volume de paquets entre toutes les sortes d'acteurs en dehors de la victime, il est peu probable que l'un d'eux remarque son implication sur la base des changements de schéma de trafic.

Tirant parti d'un serveur de noms récurrent ouvert qui prend en charge EDNS0 [RFC2671], le facteur d'amplification (taille de paquet de réponse / taille de paquet d'interrogation) pourrait être d'autour de 80. Avec ce facteur d'amplification, une relativement petite armée de clients et serveurs de noms récurrent ouverts pourrait générer des gigabits de trafic vers la victime.

Avec la longueur croissante des réponse d'autorité du DNS découlant du déploiement de DNSSEC [RFC4033] et des enregistrements de ressource NAPTR comme ceux utilisés dans les services ENUM, les serveurs d'autorité vont éventuellement être plus utiles comme acteurs dans cette sorte d'attaque d'amplification.

Même si cette attaque d'amplification n'est possible que par le non déploiement de la [RFC2827] (BCP38) il est plus facile de l'atténuer pour des raisons historiques. Quand l'Internet était une communauté beaucoup plus soudée, certaines mises en œuvre de serveurs de noms étaient disponibles avec des configurations par défaut qui, utilisées pour des serveurs de noms récurrents, rendaient le serveur accessible à tous les hôtes de l'Internet.

Pendant des années, cette configuration a été pratique et utile, permettant une plus large disponibilité des services. Comme le présent document vise à le mettre en évidence, il vaut beaucoup mieux maintenant être conscient de ses propres services de serveur de noms et se concentrer sur la livraison des services sur l'audience prévue de ces services -- que ce soit un campus universitaire, une entreprise, ou les client d'un fournisseur de services Internet. L'audience cible inclut aussi les opérateurs de petits réseaux et les gestionnaires de réseau privé qui décident de faire fonctionner des serveurs de noms dans le but d'optimiser leur service de DNS, car ils vont très probablement utiliser les configurations par défaut comme elles sont livrées par les mises en œuvre.

4. Configuration recommandée

Dans cette Section on décrit les bonnes pratiques actuelles pour faire fonctionner des serveurs de noms récurrents. Suivre ces recommandations réduirait les chances qu'un serveur de noms récurrent quelconque soit utilisé pour la génération d'une attaque par amplification.

La recommandation générique aux opérateurs de serveur de noms est d'utiliser les moyens fournis par la mise en œuvre du choix de ne fournir le service de recherche récurrente de noms qu'à des clients choisis. L'autorisation du client peut normalement être faite de plusieurs façons :

- Autorisation fondée sur l'adresse IP. L'utilisation de l'adresse IP de source des interrogations au DNS et de leur filtrage par une liste de contrôle d'accès (ACL, *Access Control List*) pour servir seulement les clients prévus. Ceci est facile à appliquer si la zone de service du serveur de noms récurrent est une gamme d'adresses IP raisonnablement fixée qui est protégée contre les usurpations externes d'adresse, normalement le réseau local.

- Choix fondé sur l'interface entrante. L'utilisation de l'interface entrante pour l'interrogation comme discriminant pour choisir quels clients vont être servis. Ceci est particulièrement applicable pour les appareils des professions libérales et travailleurs à domicile (SOHO, *Small Office, Home Office*) comme des routeurs large bande qui incluent des serveurs de noms récurrents incorporés.

- Les interrogations signées TSIG [RFC2845] ou SIG(0) [RFC2931] pour authentifier les clients. C'est une méthode moins encline à l'erreur qui permet aux opérateurs de serveurs de fournir le service à des clients qui changent fréquemment d'adresse IP (par exemple, des clients en itinérance). L'inconvénient courant de cette méthode est que très peu de mises en œuvre de résolveur de bout prennent en charge la signature TSIG ou SIG(0) des interrogations sortantes. L'utilisation effective de cette méthode implique, dans la plupart des cas, de faire fonctionner une instance locale d'un serveur de noms ou transmetteur mettant en antémémoire qui va être capable de signer avec TSIG les interrogations et de les envoyer au serveur de noms récurrent choisi.

- Pour les utilisateurs mobiles, utiliser un serveur de noms local qui met en antémémoire et fonctionnant sur l'appareil mobile ou utiliser un réseau privé virtuel avec un serveur de confiance.

Dans les serveurs de noms qui n'ont pas besoin de fournir un service récurrent, par exemple des serveurs qui sont destinés à être seulement d'autorité, supprimer complètement la récurrence. En général, c'est une bonne idée de garder séparés les services d'autorité et les services récurrents autant que faire se peut. Ceci dépend bien sûr des circonstances locales.

Même avec toutes ces recommandations, les opérateurs de réseau devraient envisager le déploiement du filtrage d'entrée [RFC2827] dans les routeurs pour empêcher l'utilisation de l'usurpation d'adresse comme moyen d'action viable. Dans les situations où des réglages de réseau plus complexes sont en place, le "filtrage d'entrée pour réseau multi-rattachement" [RFC3704] peut être une référence supplémentaire utile.

Par défaut, les serveurs de noms NE DEVRAIENT PAS offrir de service récurrent aux réseaux externes.

5. Considérations sur la sécurité

Le présent document ne crée pas de nouveau problème de sécurité pour le protocole DNS, il traite des faiblesses de ses mises en œuvre.

Le déploiement de la sécurité de transaction SIG(0) [RFC2931] devrait prendre en compte les avertissements sur les coûts de calcul de SIG(0) car il utilise le chiffrement à clé publique plutôt que les clés symétriques utilisées par TSIG [RFC2845]. De plus, l'identification des clés appropriées a besoin de mécanismes similaires à ceux du déploiement de TSIG ou autrement, l'utilisation des signatures DNSSEC [RFC4033] sur les RR KEY si ils sont publiés dans le DNS. Cela va à son tour exiger la gestion appropriée d'ancre de confiance DNSSEC.

6. Remerciements

Les auteurs tiennent à remercier de leurs utiles apports et commentaires Joe Abley, Olafur Gudmundsson, Pekka Savola, Andrew Sullivan, et Tim Polk.

7. Références

7.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2671] P. Vixie, "Mécanismes d'extension pour le DNS (EDNS0)", août 1999. *(P.S.) (Remplacée par* RFC6891)

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 2000, DOI 10.17487/RFC2845, (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

[RFC2931] D. Eastlake 3rd, "Signatures de demandes et de transactions du DNS (SIG(0))", septembre 2000. *(P.S.)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005, DOI 10.17487/RFC4033

7.2 Références pour information

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC3704] F. Baker, P. Savola, "Filtrage d'entrée pour réseaux à rattachement multiples", mars 2004. (BCP0084) (*MàJ par* RFC8704)

Adresse des auteurs

Joao Damas
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
US
mél : Joao_Damas@isc.org
URI : http://www.isc.org/

Frederico A. C. Neves
NIC.br / Registro.br
Av. das Nacoes Unidas, 11541, 7
Sao Paulo, SP 04578-000
BR
mél : fneves@registro.br
URI : http://registro.br/

Déclaration complète de droits de reproduction