SenderBase sur le dispositif de sécurité de la messagerie Cisco (ESA) est-il une autre RBL DNS ?

Contenu

[Question](#)
[Réponse](#)
[Informations connexes](#)

Question

SenderBase sur l'appliance de sécurité de la messagerie Cisco (ESA) est-elle une autre liste de blocage en temps réel DNS (RBL) ?

Réponse

SenderBase n'est pas une RBL DNS ordinaire. Dans la communauté antispam, il existe de nombreuses listes de blocage basées sur DNS. Technique développée au fil des ans, les listes de blocage basées sur DNS permettent d'ajouter une API standardisée (interface de programmation d'applications) à une base de données largement distribuée. Comme les périphériques réseau, tels que les serveurs de messagerie, ont tous une application cliente DNS intégrée (parfois appelée 'résolveur'), l'utilisation du DNS pour rechercher des informations sur les adresses IP est une opération très naturelle pour la plupart des systèmes. L'idée d'une liste de blocage basée sur DNS est de fournir un moyen facile pour une communauté d'utilisateurs largement distribuée d'interroger efficacement une liste orientée IP sans avoir à se soucier de la réplication de base de données, de l'authentification ou des API plus élaborées.

La stratégie de la plupart des listes de blocage basées sur DNS consiste à décrire une liste de blocage (par exemple, « systèmes connus pour être des relais ouverts »), puis à permettre à quiconque d'interroger la liste pour voir si une adresse IP figure sur la liste. Si l'adresse apparaît, le propriétaire de la liste affirme que l'adresse IP répond aux conditions requises pour figurer sur la liste. En d'autres termes, les listes de blocage basées sur DNS sont des réponses « oui/non », soit vous êtes sur la liste, soit vous ne l'êtes pas.

Les volontaires gèrent généralement des listes de blocage basées sur DNS (bien qu'il y en ait peu disponibles sur la base d'un abonnement payant). Ils ont aussi tendance à être très idiosyncrasiques dans leur fonctionnement. En tant que projets gérés par des bénévoles, ils sont gérés par des individus ou des groupes qui se sentent très fortement à l'égard du problème du spam et ont généralement tendance à se tromper en bloquant le courrier légitime. Les entreprises qui ont choisi d'utiliser des listes de blocage basées sur DNS les trouvent soit peu efficaces pour réduire le spam (c'est-à-dire qu'il est difficile d'accéder à la liste et que les mises à jour de la liste ne sont pas opportunes), soit elles constatent que ces listes génèrent un taux de faux positifs très élevé (c'est-à-dire qu'il est trop facile de s'inscrire sur la liste).

SenderBase a été créé pour réduire les comportements idiosyncrasiques dans les listes de blocage basées sur DNS et permettre au gestionnaire de réseau de prendre ses propres

décisions quant à l'utilisation prudente ou agressive de la liste. Avec une utilisation appropriée de SenderBase, associée aux fonctionnalités de limitation d'un ESA, le taux de faux positifs peut être considérablement réduit. En même temps, une grande partie du spam est conservée hors du réseau de l'entreprise.

Informations connexes

- Comment fonctionne SenderBase ?
- Support et documentation techniques - Cisco Systems