

Is SenderBase op Cisco Email Security Appliance (ESA) een andere DNS RBL?

Inhoud

[vraag](#)

[Antwoord](#)

[Gerelateerde informatie](#)

vraag

Is SenderBase op Cisco Email Security Appliance (ESA) nog een DNS Real-time Blackgat List (RBL)?

Antwoord

SenderBase is geen normale DNS RBL. In de anti-spam gemeenschap zijn er veel DNS-gebaseerde blokklijsten. Een techniek die in de loop der jaren is ontwikkeld, bieden DNS-gebaseerde kaslijsten een manier om een gestandaardiseerde API (applicatie-interface) toe te voegen aan een breed gedistribueerde database. Omdat netwerkapparaten, zoals mailservers, allemaal een DNS client-toepassing hebben ingebouwd (soms een 'resolver' genoemd) is het gebruiken van de DNS om informatie over IP-adressen op te zoeken een zeer natuurlijke operatie voor de meeste systemen. Het idee van een DNS-gebaseerde blocklist is om een makkelijke manier te bieden voor een breed gedistribueerde gemeenschap van gebruikers om op efficiënte wijze een IP-georiënteerde lijst te bevragen zonder zich zorgen te hoeven maken over gegevensrepletie, verificatie of meer uitgebreide API's.

De strategie van de meeste DNS-gebaseerde blokklijsten is om een of andere beschrijving van een blocklist te geven (bijvoorbeeld "systemen die bekend staan als open relays") en dan iedereen in staat te stellen om de lijst te vragen om te zien of een IP-adres in de lijst staat. Als het adres verschijnt, beweert de eigenaar van de lijst dat het IP-adres voldoet aan de kwalificaties die in de lijst staan. Met andere woorden, DNS-gebaseerde blokklijsten zijn "ja/nee"-antwoorden - u staat op de lijst of u niet.

Vrijwilligers beheren over het algemeen DNS-gebaseerde kaslijsten (hoewel er weinig beschikbaar zijn op basis van een abonnement voor betaling). Ze hebben ook de neiging zeer idiosyncratisch te zijn in hun functioneren. Als projecten die door vrijwilligers worden beheerd, worden ze uitgevoerd door individuen of groepen die zich zeer sterk voelen over het probleem van spam en die over het algemeen de neiging hebben om legitieme mail te blokkeren. Bedrijven die ervoor hebben gekozen DNS-gebaseerde blokklijsten te gebruiken, vinden deze minimaal effectief voor het verminderen van spam (dat wil zeggen, het is moeilijk om op de lijst te komen en de lijst-updates zijn niet op tijd) of ze vinden dat deze lijsten een zeer hoog vals-positief cijfer genereren (dat wil zeggen, het is te makkelijk om op de lijst te komen).

SenderBase werd gecreëerd om idiosyncratisch gedrag in DNS-gebaseerde blokklijsten te verminderen en de netwerkbeheerder in staat te stellen om hun eigen beslissingen te maken over hoe conservatief of hoe agressief ze de lijst zullen gebruiken. Met een juist gebruik van SenderBase, in combinatie met de trottingmogelijkheden van een ESA, kan het aantal valse

positieven dramatisch gedaald worden. Tegelijkertijd wordt een groot deel van spam buiten het bedrijfsnetwerk gehouden.

Gerelateerde informatie

- [Hoe werkt SenderBase?](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)