SenderBase가 Cisco ESA(Email Security Appliance)에 또 다른 DNS RBL을 사용하고 있습니까?

목차

질문

SenderBase가 Cisco ESA(Email Security Appliance)에 또 다른 DNS RBL(Real-time Blackhole List)을 기반으로 합니까?

응답

SenderBase는 일반적인 DNS RBL이 아닙니다.안티스팸 커뮤니티에는 많은 DNS 기반 차단 목록이 있습니다.지난 몇 년간 개발된 DNS 기반 차단 목록은 표준화된 API(애플리케이션 프로그래밍 인터페이스)를 널리 분산된 데이터베이스에 추가하는 방법을 제공합니다.메일 서버와 같은 네트워크 디바이스에는 모두 DNS 클라이언트 애플리케이션 내장(일명 '확인자'라고도 함)이 있으므로 DNS를 사용하여 IP 주소에 대한 정보를 찾는 것은 대부분의 시스템에서 매우 자연스러운 작업입니다.DNS 기반 차단 목록은 널리 분산된 사용자 커뮤니티가 데이터베이스 복제, 인증 또는 보다 정교한 API에 대해 걱정할 필요 없이 IP 중심 목록을 효율적으로 쿼리할 수 있는 쉬운 방법을 제공하는 것을 목적으로 합니다.

대부분의 DNS 기반 차단 목록의 전략은 차단 목록에 대한 일부 설명(예: "오픈 릴레이로 알려진 시스템")을 표시한 다음, 목록을 쿼리하여 IP 주소가 목록에 있는지 확인하는 것입니다.주소가 나타나면 목록 소유자는 IP 주소가 목록에 포함될 자격을 충족했다고 주장합니다.즉, DNS 기반 차단 목록은 "예/아니요" 응답이며, 목록에 있거나 그렇지 않습니다.

자원봉사자들은 일반적으로 DNS 기반 차단 목록을 관리합니다(유료 서브스크립션 기준으로 사용할 수 있는 항목이 거의 없음). 그들은 또한 그들의 수술에서 매우 특이하게 행동하는 경향이 있다.자원 봉사 실행 프로젝트로서, 스팸 문제에 대해 매우 강하게 느끼고 일반적으로 합법적인 메일을 차단하는데 과오가 발생하는 경향이 있는 개인이나 그룹이 이 프로젝트를 실행합니다.DNS 기반 차단 목록을 사용하기로 선택한 기업은 스팸을 줄이는 데 최소한의 효과를 얻거나(즉, 목록에 표시하기가 어렵고 목록 업데이트가 적시에 수행되지 않음) 이러한 목록이 매우 높은 오탐(즉, 목록에 표시하기가 너무 용이함)을 발생한다는 사실을 알게 됩니다.

SenderBase는 DNS 기반 차단 목록의 고유한 동작을 줄이고 네트워크 관리자가 이 목록을 얼마나 보수적인지 또는 얼마나 공격적으로 사용할 것인지에 대해 스스로 결정할 수 있도록 하기 위해 만들어졌습니다.SenderBase를 적절하게 사용하면 ESA의 조절 기능과 함께 오탐의 속도가 크게 저하될 수 있습니다.동시에, 스팸의 상당 부분이 기업 네트워크에 연결되어 있지 않습니다.

관련 정보

- SenderBase는 어떻게 작동합니까?
- 기술 지원 및 문서 – Cisco Systems