WSA Cisco Web Reputation 개요

목차

소개

이 문서에서는 Cisco WSA(Web Security Appliance)용 Cisco WBRS(Web Reputation)에 대한 개요를 제공합니다.

기고자: Josh Wolfer 및 Stephan Fiebrandt, Cisco TAC 엔지니어

WBRS 개요

WBRS는 웹 서버의 동작 및 특성을 분석하고 스팸, 바이러스, 피싱 및 스파이웨어 위협에 대한 최신 방어 기능을 제공하는 혁신적인 방법입니다.

WBRS는 악성코드 형식이 포함된 URL을 탐지하기 위해 광범위하고 다양하며 글로벌 데이터 집합에 대한 실시간 분석을 사용합니다. WBRS는 이메일 또는 웹 트래픽에서 혼합된 위협으로부터 고객을 보호하는 Cisco 보안 데이터베이스의 중요한 부분입니다.

SenderBase의 WBRS 사용

WBRS는 세계 최대의 이메일 및 웹 트래픽 모니터링 네트워크인 Cisco의 Common Security Database(SenderBase® Network)의 데이터를 활용합니다.URL의 평판에 대한 탁월한 표시인 50개 이상의 고유 매개변수를 추적합니다.정교한 보안 모델링 및 악성코드 탐지 에이전트를 통해 Cisco는 이러한 입력을 기반으로 이러한 URL을 평가합니다.

일부 매개변수는 다음과 같습니다.

- URL 분류 데이터
- 다운로드 가능한 코드가 있음
- 복잡하고 긴 EULA(End-User License Agreement) 존재
- 글로벌 볼륨 및 볼륨 변경
- 네트워크 소유자 정보
- URL 기록
- URL 사용 기간

- 바이러스/스팸/스파이웨어/피싱/파밍 블랙리스트 존재
- 인기 도메인의 URL 유형
- 도메인 등록자 정보
- IP 주소 정보

WBRS 세분화

WBRS는 광범위한 데이터 집합을 분석하고 대부분의 악성코드 탐지 애플리케이션의 바이너리 **좋은** 범주 또는 **나쁜 범주** 대신 -10에서 +10까지의 매우 세분화된 점수를 생성하기 때문에 기존 URL 블랙리스트 또는 화이트리스트와 다릅니다.이 세분화된 점수를 통해 관리자는 유연성을 높일 수 있습니다.서로 다른 WBRS 점수 범위를 기반으로 다양한 보안 정책을 구현할 수 있습니다.