향후 Umbrella 보안 개선 사항 - 새로 확인된 도메인

목차

[소개](#)

[개요](#)

[뭐하는 거야?](#)

[왜 이러는 거죠?](#)

[어떤 혜택을 누릴 수 있습니까?](#)

소개

이 문서에서는 Secure Access 및 Umbrella 서비스의 NSD(New Seen Domains) 카테고리에 대한 향후 보안 개선 사항에 대해 설명합니다.

개요

Talos Threat Research 팀이 주도하고 있는 Cisco 보안 액세스 및 Umbrella 서비스의 핵심 요소인 NSD(New Seen Domains) 카테고리의 중요한 개선 사항에 대해 알려드리게 되어 기쁘게 생각합니다.

뭐하는 거야?

보안을 강화하기 위한 지속적인 노력의 일환으로 NSD용 업데이트 시스템을 구현하여 버전 2(NSDv2)로 전환합니다. 이 새로운 반복은 소스 데이터를 대폭 확장합니다. Investigate 제품(800B 쿼리/일)을 지원하는 Passive DNS의 전체 집합이 포함되므로(현재 New Seen Domains의 통계 샘플링 방법론에 비해 향상되었습니다.

Cisco는 NSDv2를 통해 고객의 피드백과 사용량을 보다 면밀하게 반영하고 Talos Threat Research 팀의 데이터 분석 결과를 확신할 수 있도록 데이터 세트를 개선했습니다. 이 새로운 알고리즘은 새로운 등록 레벨 도메인을 발견하는 데 초점을 맞추고 공통 상위 도메인을 공유하는 여러 하위 도메인의 "노이즈"를 줄입니다.

왜 이러는 거죠?

고객 피드백을 듣고 NSD가 어떻게 저용량 도메인의 분류를 지연시켜 갑작스러운 인기 증가를 경험했을 경우 예기치 못한 결과를 초래하고 도메인에 혼란을 일으킬 수 있는지를 보여 주는 데이터를 분석했습니다. 또한 대용량 도메인을 변경하면, 예를 들어 콘텐츠 전송 네트워크에서 이름 지정 체계의 변경 사항을 도입할 때 예기치 않은 변화가 발생할 수 있습니다.

Talos Threat Research 팀은 이러한 문제를 해결하기 위해 Umbrella와 함께 NSDv2를 개발하여 새

로 발견된 도메인을 보다 안정적이고 정확하게 식별할 수 있는 시스템을 제공합니다.

어떤 혜택을 누릴 수 있습니까?

NSDv2의 향상된 기능은 다음과 같은 보안 및 운영 효율성을 염두에 두고 설계되었습니다.

- 향상된 위협 탐지: NSDv2는 나중에 악성으로 판명되는 도메인을 식별하는 속도가 최소 45% 향상되었습니다.
- 오탐 감소: 보다 정밀한 타겟 시스템으로, 정기적으로 사용되는 부정확하게 플래그가 지정된 도메인에서 발생할 수 있는 중단을 줄일 수 있습니다.
- 최적화된 성능: 간소화된 데이터 세트를 통해 더 신속하게 게시할 수 있을 뿐만 아니라 지원 팀이 문제가 발생할 경우 신속하게 해결할 수 있습니다.
- 시행 '모범 사례': 이 범주는 더 일관성 있고 관련성이 높으며 업계 및 고객의 기대에 더 잘 부합할 수 있습니다.
- 강화된 보고 데이터: NSDv2의 향상된 컨텍스트 및 커버리지는 보고서의 데이터를 강화합니다.
- 향상된 예측: 이 업데이트는 Intelligent Proxy가 심층 검사가 필요한 위험한 도메인을 판별하는 데 도움이 됩니다.
- 고객 상호 작용 불필요: 이는 동적 범주화를 위한 파이프라인의 업데이트이며, 고객을 위한 마이그레이션 또는 정책 변경이 필요하지 않습니다. 이는 관리자 및 최종 사용자를 위해 완벽하게 투명하게 개선되었습니다.

이 카테고리에 대한 변경 사항은 2024년 8월 13일에 구축됩니다. 당사의 서비스에 대한 귀하의 지속적인 신뢰에 감사드리며 이러한 중요한 보안 개선 사항을 귀사에 제공하고자 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.