Umbrella에서 새로 확인된 도메인 보안 범주 활성화

목차

소개

이 문서에서는 Cisco Umbrella의 "새로 확인된 도메인"(NSD) 보안 카테고리에 대해 설명합니다.

배경 정보

NSD(New Seen Domains)는 지난 24시간 동안 Cisco Umbrella DNS 서비스(가정용 사용자를 위한 무료 OpenDNS 서비스 포함) 사용자가 처음으로 쿼리한 도메인을 식별하는 보안 카테고리입니다. 이 보안 범주는 다른 보안 범주와 동일하게 작동하며 기존 보안 설정 또는 새 보안 설정의 일부로 활성화할 수 있습니다. 도메인은 24시간 동안 목록에 남아 있습니다.

Cisco Umbrella에서 도메인을 "새로 표시"하는 방법

새로운 도메인은 새로운 악성코드 캠페인의 일부로 생성되는 경우가 많습니다. 기존의 시그니처 기반 방식으로는 알려진 악성 웹 사이트를 차단하는 것을 인식하지 못하기 때문에 이러한 캠페인을 진행하는 악의적인 사용자는 새로운 도메인을 사용합니다. 예를 들어, 피싱 캠페인에서는 사용자에게 링크를 클릭하도록 권유하는 주요 스팸 캠페인과 동반할 새 도메인을 만들 수 있습니다. 이 링크는 아직 이 캠페인의 일부로 알려져 있지 않으며 알려진 악성 도메인의 표준 목록에 의해 차단되지 않습니다. 이러한 목록에 링크가 추가되기 전에 범죄자는 데이터를 유출하고, 악성코드를 설치하고, 네트워크 액세스를 얻을 수 있는 충분한 시간을 갖게 됩니다.

NSD(New Seen Domains) 보안 카테고리는 이전에 본 적이 없는 도메인 조회에 대해 DNS 로그를 확인하여 작동합니다. 잘못된 쿼리의 볼륨 때문에 도메인이 새로 표시된 것으로 표시되려면 클라이언트 쿼리가 적절한 응답을 받아야 합니다. 도메인이 처음 발견되면 24시간 동안 목록에 추가됩니다. 이 기간이 지나면 도메인이 더 이상 새로 표시되지 않으며 목록에서 제거됩니다.

쿼리할 때 도메인이 속한 범주가 보고서에 기록됩니다. 따라서 도메인을 쿼리할 때 새로 표시된 것으로 분류한 경우 활동 검색 또는 보안 활동 보고서에서 보고합니다. 그러나 도메인이 목록에서 만료되면 해당 도메인에 대한 현재 데이터를 기준으로 도메인을 피벗하면(특히 새 대상 또는 ID 보고

서, Investigate Console 또는 Investigate API 사용) 해당 도메인이 더 이상 새로 표시되지 않습니다. 다시 말해, 며칠 후에 도메인을 다시 방문하면 Umbrella에 새로 표시된 것처럼 더 이상 표시할 수 없습니다. 이것은 설계에 의한 것이지만 약간의 초기 혼동을 초래할 수 있습니다.

Newly Seen Domain의 유일한 정의는 다음과 같습니다. 그것은 새롭게 보입니다. 따라서 새로 확인된 것으로 분류된 도메인 중 상당수는 악성이 아니며, 이 보안 카테고리에서 합법적인 도메인 탐지가 발생할 것으로 예상됩니다. 특히 콘텐츠를 제공하기 위해 무작위 하위 도메인을 생성하는 Akamai 및 Cloudfront와 같은 특정 서비스 및 CDN에 대한 예방 조치가 구현되어 있습니다. Facebook이나 Google과 같이 널리 사용되는 도메인에 대한 기존의 보증도 이러한 도메인이 포함되지 않도록 하기 위해 사용되었습니다.

또한 정규화된 도메인 이름(두 번째 수준 도메인 또는 두 번째 수준 도메인의 하위 도메인)만 새로 표시되는 도메인으로 간주됩니다. 최상위 도메인 및 국가 코드 최상위 도메인은 대규모 도메인 그룹을 차단하는 것을 방지하기 위해 Newly Seen Domains에 포함되지 않습니다.

구현에 대한 중요 참고 사항

원치 않는 탐지가 발생할 수 있으므로 Cisco Umbrella는 이 보고서를 감사 모드 또는 차단 또는 조치 없이 탐지만 모드에서 사용할 것을 적극 권장합니다. 기본적으로 보안 설정에서 이 범주를 사용할 수 있는 모든 사용자는 Newly Seen Domains(새로 확인된 도메인)를 보고서에서 탐지된 도메인으로 간주합니다. 이는 기능이 기본적으로 차단 없이 활성화됨을 의미합니다. 대부분의 경우, 사용자는 보고서를 사용하여 어떤 트래픽이 카테고리와 일치하는지 확인하고, 해당 정보를 사용하여 이러한 도메인을 더 심층적으로 조사하여 자동으로 차단하는 대신 잠재적으로 보안 위협을 나타낼 수 있는지를 확인해야 합니다.

또 다른 주요 주의 사항은 도메인에 대한 첫 번째 쿼리가 허용된다는 것입니다. 이는 Cisco Umbrella가 이전에 해당 도메인에 대한 쿼리를 본 적이 없기 때문에 로깅 시스템에서 Newly Seen Domains 카테고리의 일부로 포함하도록 처리되지 않았기 때문입니다. 도메인을 처음 쿼리할 때와 해당 카테고리와 일치하는 도메인 목록에 나타나기 전의 시간 간격은 약 5분이지만 이를 초과할 수 있습니다. Cisco Umbrella가 처리 시간 및 볼륨으로 인해 DNS 쿼리 로그를 100% 처리할 필요는 없기 때문입니다.

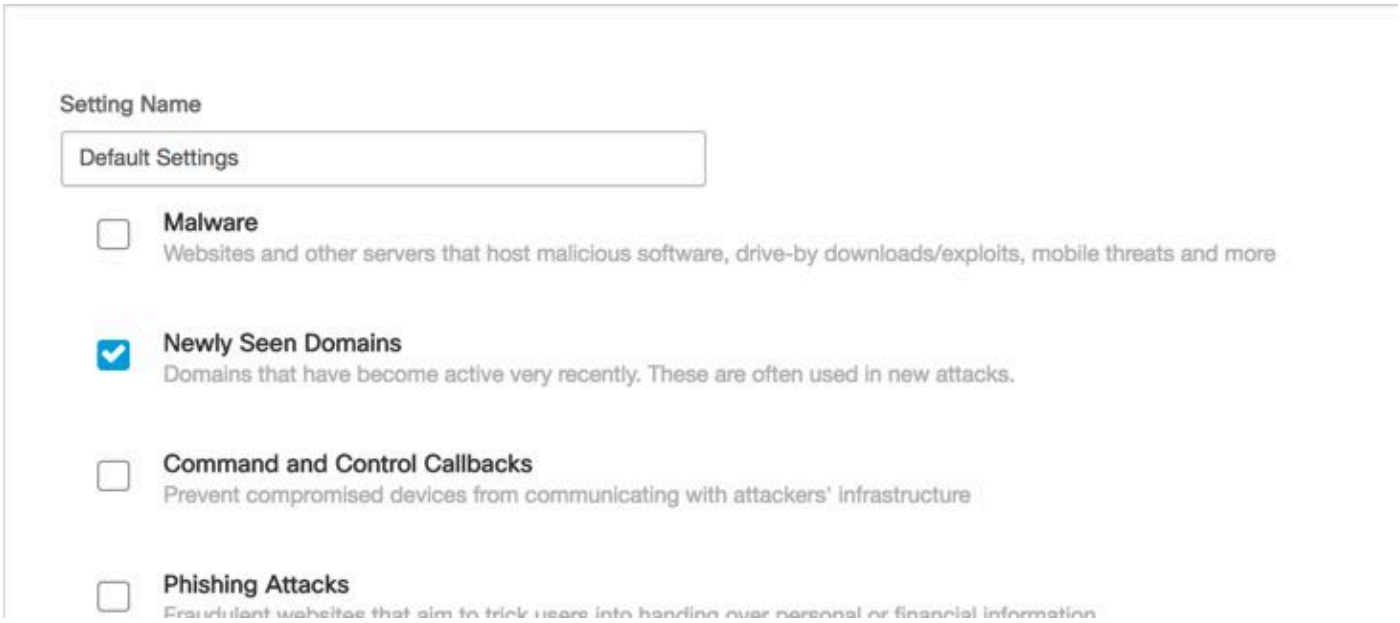
새로 확인된 도메인 프록시

Umbrella Intelligent Proxy를 사용하는 고객은 NSD 카테고리의 일부 도메인이 프록시되는 것을 관찰할 수도 있습니다. 이것은 설계에 의한 것입니다. Umbrella Labs 팀은 이러한 새 도메인을 프록시하여 수집한 데이터를 사용하여 악성코드 범주에 즉시 추가할 수 있는지 여부를 확인합니다. 이로 인해 프록시되는 Newly Seen 도메인으로 전송된 비표준 트래픽이 프록시 레벨에서 삭제되는 부작용이 있습니다. 지능형 프록시는 일반적으로 웹 트래픽에 사용되는 포트인 포트 80 및 443만 프록시합니다. 이는 카테고리의 차단 여부와 상관없이 프록시가 활성화된 경우 자동으로 발생합니다. 새로 표시된 단일 도메인이 프록시되지 않도록 하려면 해당 허용 목록에 추가합니다.

Intelligent Proxy에 대한 자세한 내용은 설명서 Enable the Intelligent Proxy를 참조하십시오.

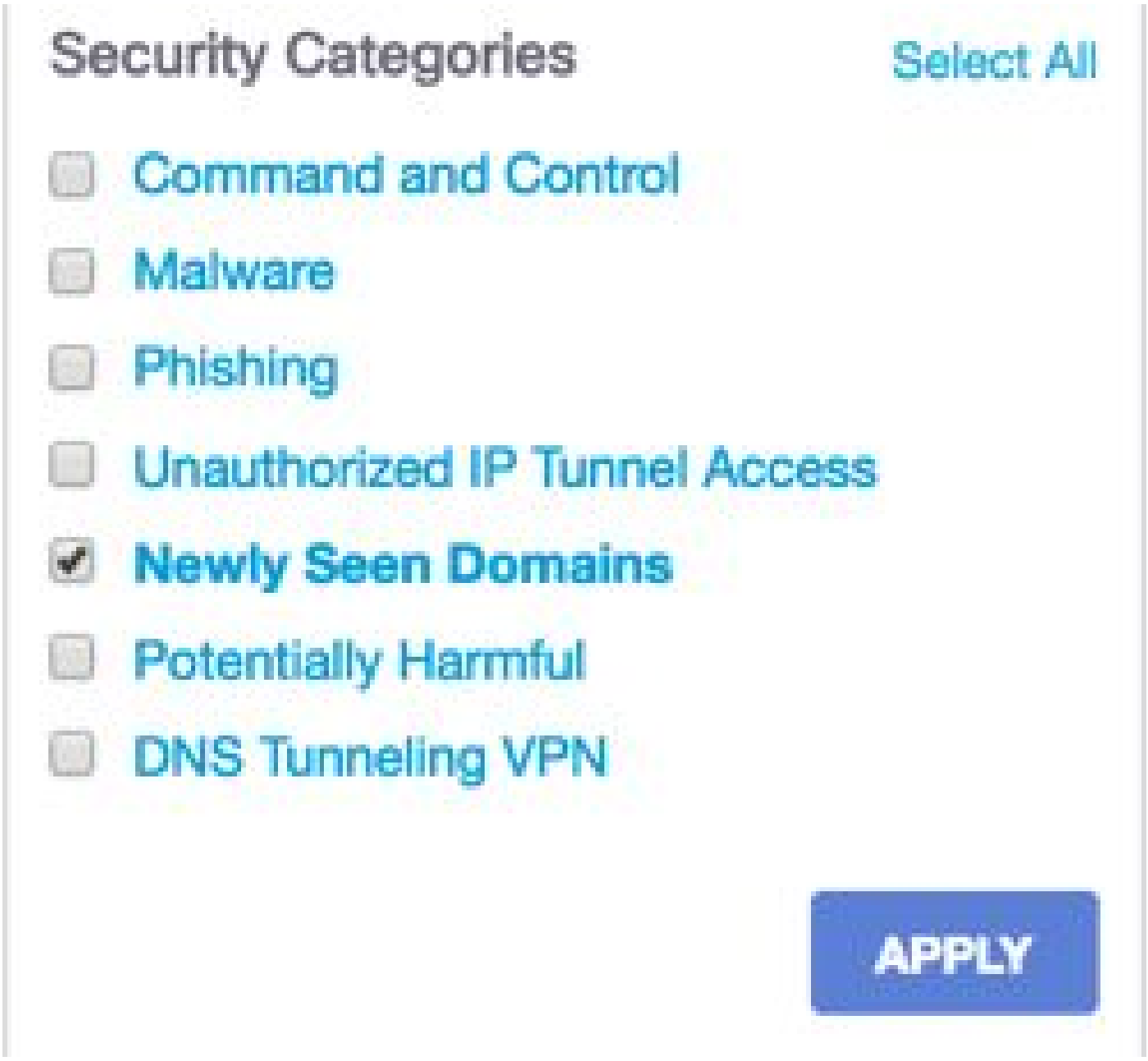
새로 본 도메인 활성화

새로 표시된 도메인 보안 범주는 정책 > 보안 설정에서 다른 범주와 마찬가지로 활성화한 다음 기존 보안 설정을 편집할 수 있습니다. 또는 정책 구성 마법사 자체 내에서 수행할 수도 있습니다.



115014822286

Activity Search와 같은 특정 보고서에 대해 새로 표시된 도메인을 필터링할 수도 있습니다.



115015007423

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.