Cisco WSA 랜섬웨어 탐지 기능 및 AMP 통합 확인

목차

문제

Cisco WSA(Secure Web Appliance)에서 Triple X Ransomware에 대한 특정 시그니처 또는 탐지 기능을 제공하는지 여부를 문의했습니다. 이 질문에는 AMP(Advanced Malware Protection)와 Cisco Talos Threat Intelligence의 통합이 WSA 플랫폼에서 올바르게 작동하고 있는지 확인하는 방법에 대한 설명 요청도 포함되었습니다.

환경

- Cisco WSA(Secure Web Appliance)
- AMP(Advanced Malware Protection) 통합
- Cisco Talos 위협 인텔리전스 통합
- 웹 평판 및 URL 필터링(WBRS)
- 안티멀웨어 스캐닝 엔진(Webroot, McAfee, Sophos)
- AVC(Application Visibility and Control)

해결

Cisco Secure Web Appliance는 Triple X Ransomware를 위해 특별히 명명된 단일 전용 시그니처를 사용하지 않습니다. 대신 WSA는 다양한 탐지 기술을 활용하여 Triple X Ransomware 변형을 비롯한 랜섬웨어 위협을 식별하고 차단하는 포괄적인 멀티 레이어 보안 아키텍처를 사용합니다.

WSA 탐지 방법

WSA 플랫폼은 랜섬웨어 보호를 위해 다음과 같은 탐지 기술을 사용합니다.

- 패턴 일치 알고리즘
- 휴리스틱 분석
- 에뮬레이션 기술
- Cisco Talos 위협 인텔리전스와 통합된 AMP(Advanced Malware Protection)
- 웹 평판 및 URL 필터링(WBRS)
- Webroot, McAfee, Sophos를 비롯한 여러 안티멀웨어 스캐닝 엔진
- AVC(Application Visibility and Control)

이러한 탐지 기능은 새로운 위협에 대한 보호를 보장하기 위해 몇 분마다 배포되는 새로운 규칙으로 지속적으로 업데이트됩니다.

AMP 및 Talos 통합 확인

AMP(Advanced Malware Protection)와 Cisco Talos Threat Intelligence의 통합이 WSA에서 제대로 작동하는지 확인하기 위해 관리자는 다음 로그를 검토할 수 있습니다.

1단계: WSA 액세스 로그 검토

WSA 어플라이언스의 액세스 로그를 검토하여 AMP 판정이 다운로드된 파일 및 웹 요청에 적용되는지 확인합니다.

2단계: AMP 로그 확인

AMP 로그를 검토하여 악성코드 분석 결과 및 위협 인텔리전스 데이터가 처리되는지 확인합니다.

3단계: WBRS 점수 확인

WBRS(Web Reputation) 점수가 채워지고 있으며 이 점수가 로그의 웹 요청과 연결되어 있는지 확인합니다.

AMP 판정 및 WBRS 점수가 로그에 채워지고 적용되는 경우, 이는 AMP와 Talos 통합이 예상대로 작동하며 실시간 위협 인텔리전스 기반 결정을 제공함을 나타냅니다.

원인

이는 트러블슈팅이 필요한 기술적 문제가 아닌 WSA 랜섬웨어 탐지 기능에 대한 정보 요청이었습니다. WSA가 특정 랜섬웨어 변종으로부터 어떻게 보호하는지 파악하고 위협 인텔리전스 통합이 제대로 작동하고 있는지 확인하려는 요구에서 이러한 질문이 제기되었습니다.

관련 콘텐츠

- Cisco Secure Web Appliance의 기능 및 이점
- Cisco Talos 위협 인텔리전스 서비스
- Cisco Secure Web Appliance 데이터시트
- Cisco 기술 지원 및 다운로드

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.