보안 웹 어플라이언스 및 AMP(Advanced Malware Protection) 로그 문제 해결(앰퍼런스)

목차

소개

이 문서에서는 WSA(Web Security Appliance)의 AMP(Advanced Malware Protection) 엔진**의 INFO** 및 **DEBUG** 로그 레벨에 있는 악성코드 판정 섹션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 설치된 WSA
- 파일 평판 및 파일 분석 사용
- AMP
- Cisco Secure Web Appliance
- SSH 클라이언트

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

WSA는 AMP for Endpoints 및 로컬 AMP 엔진과의 통합을 제공합니다. AMP는 파일 평판 및 파일 분석 기능을 통해 제로데이 악성코드로부터 악성코드를 보호합니다. WSA에는 퍼블릭 클라우드 검사 전에 내부적으로 파일 스캔을 담당하는 사전 분류 엔진이 포함되어 있습니다. 다음 섹션에서 설명하는 로그는 AMP 클라우드 또는 Threat Grid가 아닌 WSA의 AMP 엔진과 관련이 있습니다.

WSA AMP 로그 트러블슈팅

AMP 로그에 액세스합니다. CLI를 통해 로그인하거나 amp 로그를 크게 클릭합니다.

1. SSH 클라이언트를 통해 **CLI**에 로그인합니다.

2. grep 명령을 입력하고 **Enter** 키를 **누릅니다**.

3. 주문에 따라 **amp_logs**의 번호를 입력합니다.

4. 다음 옵션에 응답합니다(라이브 트래픽을 실행하는 경우 로그를 **미세**로 지정하는 옵션을 선택합니다).
5. **Enter** 키를 누릅니다.

6. 로그가 표시됩니다.

WSA AMP 로그는 다양한 정보 레벨에 있으며 다음 섹션에서 설명한 약간 다른 결과를 **INFO** 레벨 **또는** DEBUG를 선택할 수 있습니다.

> **참고:** AMP 로그를 선택하려면 AMP 라이센스를 WSA에 설치해야 합니다.

AMP 정보 레벨 로그:

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated
memory = 0, AMP used memory = 0, Scans in flight = 1, Active faster connections = 1, Active
slower connections = 0
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]:
filename[npp.8.4.Installer.x64.exe] filemime[application/x-dosexec] file_extension[exe]
length[4493047b] ampverdict[(1, 1, 'amp', '', 0, 0, True)] scanverdict[0] malwareverdict[0]
spyname[] SHA256[ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1] From[Cloud]
uploadreason[Enqueued in the local queue for submission to upload] verdict_str[FILE UNKNOWN]
is_slow[0] scans_in_flight[0] Active faster connections[0] Active slower connections[0]
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server:
https://panacea.threatgrid.com, SHA256:
ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1, Filename:
npp.8.4.Installer.x64.exeTimestamp: 1651044116 sampleid[]
```

AMP INFO 레벨 로그(앰프):

```
ampverdict[(1, 1, 'amp', '', 0, 0, True)]
(analysis_Action, scan_verdict, ‘verdict_source', ‘spyname’, malware_verdict, file_reputation,
upload_action)]
```

AMP 디버그 레벨 로그:

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b]
readtime[109.721680ms] scantime[2.205322ms] ampverdict[(1, 1, 'amp', '', 0, 0, False)]
scanverdict[0] malwareverdict[0]
SHA256[e7a2345c75a03e63202b12301c29bb8b6bae7cef9e191ed58797ec028def7c4f] From[Cloud]
FileName[favicon.ico] FileMime[application/octet-stream]
```

AMP DEBUG 레벨 로그(샘플):

```
ampverdict[(1, 1, 'amp', '', 0, 0, False)]
ampverdict[(analysis_action, scan_verdict,disposition, ‘spyname: policy name if amp registered
with console’, file_reputation, upload_action, ‘sha256', ‘threat_name’)]
```

세부 필드 및 값 옵션:

필드	가치
분석_작업	"0"은 Advanced Malware Protection이 분석을 위해 파일 로드를 요청하지 않았음을 나타냅니다. "1"은 Advanced Malware Protection이 분석을 위해 파일 로드를 요청했음을 나타냅니다.
스캔_판정	0: 파일이 악성이 아닙니다. 1: 파일 형식 때문에 파일이 검사되지 않았습니다. 2: 파일 스캔 시간이 초과되었습니다. 3: 스캔 오류 3개 이상: 파일이 악의적임
판정_원본	amp: 파일 분석
처리	1: 알 수 없음 2: 청소 3: 악성(amp) 4: 검사 불가(검사 불가)
스파이이름	비어 있음: AMP 보안 침해 정책이 사용되지 않는 경우 Simple_Custom_Detection: AMP 보안 침해 정책이 사용되는 경우
업로드_작업	참: 파일을 샌드박스로 설정 거짓: 파일이 샌드박스로 전송되지 않음
SHA256	SHA256
위협_이름	AMP 위협 유형 기반 위협 이름

관련 정보

- AMP for Endpoints 및 Threat Grid를 WSA와 통합
- 파일 평판 필터링 및 파일 분석
- 기술 지원 및 문서 - Cisco 시스템