Probleemoplossing bij beveiligde webapplicatie en Advanced Malware Protection Logs (ampversie)

Inhoud

Inleiding

In dit document wordt het onderdeel Amverdict beschreven in het logniveau **INFO** en **DEBUG** van de Advanced Malware Protection (AMP)-motor van Web Security Appliance (WSA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Geïnstalleerd WSA
- Toetsing en bestandsanalyse ingeschakeld
- Advanced Malware Protection
- Cisco Secure Web Appliance
- SSH-client

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

WSA biedt integratie met AMP voor Endpoints en een lokale AMP-motor. AMP biedt bescherming tegen malware op nul dagen tegen malware door de bestands reputatie en bestandanalyse-

functies. De WSA omvat een pre-classificatie motor die verantwoordelijk is voor interne bestandsscans vóór openbare wolkencontroles. De in de volgende sectie beschreven logboeken zijn gerelateerd aan de AMP-motor op WSA, niet aan de AMP-wolk of Threat Grid.

Vastlegging probleemoplossing WSA-AMP's

Toegang tot de AMP-logboeken. Meld u aan via CLI en staart of breek het postzegel:

1. Meld u aan bij de **CLI** via de SSH-client.

2. Typ de **opdrachtregel** en druk op **de** toets **ENTER**.

3. Voer het nummer van de **amp_logs in** zoals deze opdracht is gegeven.

4. Beantwoord de volgende opties (Als u live verkeer gebruikt, hebt u de optie **staart** op de logbestanden).
5. Druk op **ENTER**-toets.

6. Aantekeningen worden weergegeven.

WSA AMP-logboeken bestaan in verschillende niveaus van informatie, u kunt het **INFO-**niveau selecteren of de resultaten **DEBUG** die kleine verschillen in de volgende sectie verklaren.

> **Opmerking:** AMP-licentie moet op WSA worden geïnstalleerd om de AMP-logbestanden te selecteren.

Meldingen op AMP-INFO-niveau:

```
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[]
```

Blogs met AMP-INFO-niveau (ampverdict):

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

Op AMP DEBUG-niveau staat:

```
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]
```

Logboeken op AMP DEBUG-niveau (ampverdict):

```
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’)]
```

Gedetailleerde veld vs waardeopties:

Veld	Waarde
Analyse_actie	"0" geeft aan dat Advanced Malware Protection niet om bestand voor analyse heeft gevraagd "1" geeft aan dat Advanced Malware Protection heeft gevraagd het bestand voor analyse te uploaden
Scannen_vonnis	0: Het bestand is niet kwaadaardig 1: Het bestand is niet gescand vanwege het bestandst 2: Time out bestand 3: Scanfout Meer dan 3: Bestand is kwaadaardig
Verdict_source	amp: bestandsanalyse
ontbinding	1: Onbekend 2: Reinigen 3: Malicious (amp) 4: Niet scannbaar (niet scannbaar)
Spyname	Leeg: als het uitbraakbeleid van AMP niet wordt gebru Simple_Custom_Detection: indien een uitbraakbeleid v AMP wordt gebruikt
Upload_action	Waar: bestand is op sandbox ingesteld Onjuist: bestand wordt niet naar de sandbox verzonde
Sha256	SHA256
Threat_name	Bedreigingsnaam op basis van dreigingstypen voor AM

Gerelateerde informatie

- Advanced Malware Protection voor endpoints en Threat Grid met WSA
- Filtering van bestanduploaden en bestandsanalyse
- Technische ondersteuning en documentatie - Cisco Systemen