Fehlerbehebung für sichere Web-Appliance und erweiterte Malware-Schutzprotokolle (Ampverdict)

Inhalt

Einleitung

Dieses Dokument beschreibt den Abschnitt "Ampverdict" in der **INFO**- und **DEBUG**-Protokollstufe der AMP-Engine (Advanced Malware Protection) der Web Security Appliance (WSA).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- WSA installiert
- Dateireputation und Dateianalyse aktiviert
- Advanced Malware Protection
- Cisco Secure Web Appliance
- SSH-Client

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die WSA ermöglicht die Integration mit AMP für Endgeräte und einer lokalen AMP-Engine. AMP bietet Malware-Schutz durch Dateireputation und Dateianalysefunktionen. Die WSA enthält eine

Vorabklassifizierungs-Engine, die für interne Dateiprüfungen vor Public Cloud-Prüfungen verantwortlich ist. Die im nächsten Abschnitt beschriebenen Protokolle beziehen sich auf die AMP-Engine der WSA, nicht auf die AMP-Cloud oder Threat Grid.

Fehlerbehebung bei WSA AMP-Protokollen

Zugriff auf die AMP-Protokolle Melden Sie sich über CLI an, und schalten Sie die AMP-Protokolle ein, oder fett Sie sie an:

1. Melden Sie sich über den SSH-Client bei der **CLI an**.

2. Geben Sie den Befehl **grep ein** und drücken die **Eingabetaste**.

3. Geben Sie die Nummer des **AMP_LOS** wie bestellt ein.

4. Beantworten Sie die folgenden Optionen (Wenn Sie Live-Datenverkehr ausführen, wählen Sie die Option zum **Umschalten** der Protokolle aus).
5. Drücken Sie die **Eingabetaste**.

6. Protokolle werden angezeigt.

WSA-AMP-Protokolle existieren in verschiedenen Informationsebenen. Sie können die **INFO-**Ebene auswählen oder **DEBUG** die Ergebnisse auswählen, die geringfügige Unterschiede aufweisen, die im nächsten Abschnitt erläutert werden.

> **Anmerkung:** Die AMP-Lizenz muss auf der WSA installiert werden, um die AMP-Protokolle auszuwählen.

Protokolle der AMP-INFO-Ebene:

```
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-Stufenprotokolle (Ampverdict):

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

Protokolle der AMP-DEBUG-Ebene:

```
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-Stufenprotokolle (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’)]
```

Optionen für detaillierte Felder und Werte:

Feld	Wert
Analyse_Aktion	"0" bedeutet, dass Advanced Malware Protection den Upload der Datei nicht zur Analyse angefordert hat. "1" gibt an, dass Advanced Malware Protection den Up der Datei zur Analyse angefordert hat
Scan_Verdict	0: Die Datei ist nicht schädlich 1: Die Datei wurde wegen ihres Dateityps nicht gescan 2: Zeitüberschreitung bei Dateiprüfung 3: Scan-Fehler Mehr als 3: Datei ist schädlich
Verdict_Source	AMP: dateianalyse
Disposition	1: Unbekannt 2: Löschen 3: Schädlich (AMP) 4: Nicht scanbar (nicht scanbar)
Spyname	Leer: Wenn die AMP-Outbreak-Richtlinie nicht verwen wird Simple_Custom_Detection: Wenn eine AMP-Outbreak- Richtlinie verwendet wird
Upload_Action	Richtig: Datei ist auf Sandbox eingestellt Falsch: Datei wird nicht an die Sandbox gesendet
Sha256	SHA256
Bedrohungsname	Bedrohungsname basierend auf AMP-Bedrohungstype

Zugehörige Informationen

- Integration von AMP für Endgeräte und Threat Grid mit der WSA
- Dateireputations-Filterung und Dateianalyse
- Technischer Support und Dokumentation - Cisco Systeme