セキュアなWebアプライアンスと高度なマルウェア防御ログのトラブルシューティング(ampbdict)

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[WSA AMPログのトラブルシューティング](#)
[関連情報](#)

概要

このドキュメントでは、Webセキュリティアプライアンス(WSA)の高度なマルウェア防御(AMP)エンジンの**情報(INFO)**および**デバッグ(DEBUG)**ログレベルのampvertiseセクションについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WSAがインストールされました
- ファイルレピュテーションとファイル分析が有効
- 高度なマルウェア防御
- Cisco Secure Webアプライアンス
- SSH client

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

WSAは、エンドポイント用AMPおよびローカルAMPエンジンとの統合を提供します。AMPは、ファイルレピュテーションおよびファイル分析機能を通じて、ゼロデイマルウェアに対するマルウェア防御を提供します。WSAには事前分類エンジンが含まれており、パブリッククラウドチェックの前に内部でファイルスキャンを実行します。次のセクションで説明するログは、AMPクラウドまたはThreat Gridではなく、WSAのAMPエンジンに関連しています。

WSA AMPログのトラブルシューティング

AMPログにアクセスします。CLIを使用してログインし、ampログをtailまたはgrepします。

1. SSHクライアントを介して**CLIにロ**グインします。

2. grepコマンドを入力**し、Enter**キーを**押し**ます。

3.注文時の**amp_logsの数**を入力します。

4.次のオプションに答えてください(ライブトラフィックを実行する場合は、ログの末尾にオプション**を選択**してください)。
5. Enterキーを**押し**ます。

6.ログが表示されます。

WSA AMPログは異なるレベルの情報に存在します。次のセクションで説明する若干の違いを持つ**情報**レベルまたは**デバッグ**結果を選択できます。

> **注：**AMPログを選択するには、AMPライセンスをWSAにインストールする必要があります。

AMP INFOレベルのログ：

```
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レベルのログ（判定）：

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

AMPデバッグレベルのログ：

```
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デバッグレベルのログ(ampbechation):

```
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’)]
```

詳細フィールドと値オプション：

フィールド	値
Analysis_action	「0」は、Advanced Malware Protectionが分析のため ァイルのアップロードを要求しなかったことを示しま 「1」は、Advanced Malware Protectionが分析のため ァイルのアップロードを要求したことを示します
スキャン_判定	0：ファイルに悪意はありません 1:ファイルの種類が原因で、ファイルはスキャンされ んでした 2:ファイルスキャンがタイムアウトしました 3：スキャンエラー 3より大きい：ファイルが悪意がある
Verdict_source	amp:ファイル分析
評価	1:[不明（Unknown）] 2:クリーン 3：悪意のある(amp) 4：スキャン不可（スキャン不可）
スパイネーム	空:AMPアウトブレイクポリシーが使用されていない場 Simple_Custom_Detection:AMPアウトブレイクポリシ 使用されている場合
Upload_action	True：ファイルはsandboxに設定されます False:sandboxにファイルが送信されない
Sha256	SHA256
Threat_name	AMP脅威タイプに基づく脅威名

関連情報

- エンドポイント向けAMPとThreat GridのWSAとの統合
- ファイルレピュテーションフィルタリングとファイル分析
- テクニカルサポートとドキュメント – シスコ システム