AMPを使用するESAのアラート「Upload Limit Reached」について理解する

内容

概要

このドキュメントでは、高度なマルウェア防御(AMP)機能を使用して電子メールをスキャンするように設定されている場合に、Eメールセキュリティアプライアンス(ESA)がスローするアラート「Upload Limit Reached」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。

- E メール セキュリティ アプライアンス
- 高度なマルウェア防御

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア12.xを実行するEメールセキュリティアプライアンス(ESA)

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

Eメールセキュリティアプライアンス(ESA)は、高度なマルウェア防御(AMP)機能を使用します。この機能には、次の2つの主な機能があります。

- ファイルレピュテーション
- ファイル分析

File Analysisは、サンドボックス分析用のメッセージ添付ファイルをThreatGridクラウドサーバにアップロードします。

「Upload Limit Reached」アラートについて

メッセージトラッキングでは、Advanced Malware Protection(AMP)がアップロード制限に達したため、Eメールがスキャンされなかったことが示されます。

例：

```
02 Dec 2019 14:11:36 (GMT +01:00) Message 12345 is unscannable by Advanced Malware Protection engine. Reason: Upload Limit Reached
```

新しいThreatGridサンプル制限モデルでは、これらの制限は組織ごとにデバイスがファイル分析のためにアップロードできるサンプルの数です。すべての統合デバイス(WSA、ESA、CES、FMCなど)およびエンドポイント用AMPは、デバイスの数に関係なく、1日あたり200サンプルを使用できます。

これは共有制限（デバイスごとの制限ではありません）であり、2017年12月1日以降に購入したライセンスに適用されます。

> **注：**このカウンタは毎日リセットされるのではなく、24時間のロールオーバーとして機能します。

例：

アップロードサンプル数が200に制限されている4つのESAのクラスタで、ESA1が今日の10:00に80のサンプルをアップロードした場合、今日の10:01から明日の10:00まで、最初の80スロットがリリースされるまでの4つのESA（共有制限）の中で、さらに120のサンプルのみをアップロードできます。

過去24時間にESAがアップロードしたサンプル数を確認する方法

ESA:[Monitor] > [AMP File Analysis] レポートに移動し、[Files Uploaded for Analysis] セクションをオンにします。

SMA:[Email] > [Reporting] > [AMP File Analysis] レポートに移動し、[Files Uploaded for Analysis] セクションをオンにします。

> **注：**AMPファイル分析レポートに正確なデータが表示されない場合は、ユーザガイドの「クラウドのファイル分析の詳細が不完全」セクションを参照してください。

> **警告：**詳細については、不具合CSCvm10813を参照してください。

あるいは、CLIからgrepコマンドを実行して、アップロードされたファイルの数をカウントすることもできます。

これは各アプライアンスで実行する必要があります。

例：

```
grep "Dec 20.*File uploaded for analysis" amp -c
grep "Dec 21.*File uploaded for analysis" amp -c
```

PCRE正規表現を使用して日時を照合できます。

アップロードの制限を拡張する方法

シスコ内のアカウントマネージャまたはセールスエンジニアに連絡してください。

関連情報

- AMPとThreat GridのCisco Eメールセキュリティとの統合の詳細
- ESAでのファイル分析アップロードの確認
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。