ESA の Advanced Malware Protection（AMP）のテスト

内容

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス（ESA）の高度なマルウェア防御（AMP）機能をテストして確認する方法について説明します。

ESA 上での AMP のテスト

ESA 用の AsyncOS 8.5 のリリースを使用する AMP は、ファイル レピュテーション スキャンとファイル分析を実行して、添付ファイル内のマルウェアを検出します。

機能キー

AMP を実装するには、ESA 上での**ファイル レピュテーションとファイル分析の両方に対して有効でアクティブな機能キーが必要です。**GUI で [System Administration] > [Feature Keys] **にアクセスするか、CLI で featurekeys を使用して機能キーを確認します。**

セキュリティ サービス

GUI からサービスを有効にするには、[Security Services] > [File Reputation and Analysis] に移動

します。CLI からは、**ampconfig** を実行することができます。設定に対する変更を送信してコミットします。

受信メール ポリシー

サービスを有効にしたら、そのサービスを受信メール ポリシーに対応付ける必要があります。

1. [Mail Policies] > [Incoming Mail Policies] に移動します。
2. 必要に応じてデフ**ォルトのポリシー**または構成済みのポリシーを選択します。[受信メール ポリシー]ページの[高度なマルウェア防御]列が表示されます。
3. その列の [Disabled] **リンクを選択し、オプション ページで [Enable File Reputation] と [Enable File Analysis] を選択します。**
4. 必要に応じて、メッセージ スキャン、スキャン不能の添付ファイルに対するアクション、および肯定的に識別されたメッセージに対するアクションで設定を拡張することができます。
5. 設定に対する変更を送信してコミットします。

テスト

現時点で、マルウェアをスキャンして検出するための受信メール ポリシーが有効になっています。テストする本物のマルウェア サンプルを用意する必要があります。有効なサンプルが必要な場合は、「European Institute for Computer Antivirus Research（eicar）」ダウンロード ページを参照してください。

> **注意**：これらのファイルまたはお客様のAVスキャナを上記のファイルと組み合わせて使用すると、コンピュータまたはネットワーク環境に損傷が発生する場合、シスコは責任を負いません。これらのファイルは、ご自身の責任でダウンロードしてください。AVスキャナ、コンピュータの設定、およびネットワーク環境の使用において十分なセキュリティが確保されている場合にのみ、ダウンロードしてください。この情報はテストや再現の目的に対して適用されます。

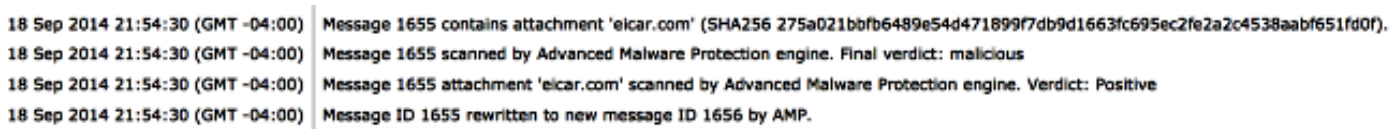
事前設定の有効な電子メール アカウントを使用している場合は、ESA と通常の処理を通して添付ファイルを送信します。ESA の CLI を使用して **mail_logs を追跡することによって、メールの処理をモニタすることができます。**メール ログに記録されたメッセージ ID（MID）を確認します。 出力は次のようになります。

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
```

```
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message-ID '<BLU437-SMTP10E1315A60354F2
906677B9DB70@phx.gbl>'
Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update''
Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
<joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine:
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp
Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

上の例は、AMP がマルウェアの添付ファイルを検出し、デフォルト設定に基づく最終アクションとして**ドロップしたことを示しています。**

同じ詳細が GUI からのメッセージ トラッキングにも表示されます。



[Incoming Mail Policies] から肯定的に識別されたマルウェアまたは AMP 設定内のその他の高度なオプションを配信すると、そのメール処理結果を確認することができます。

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

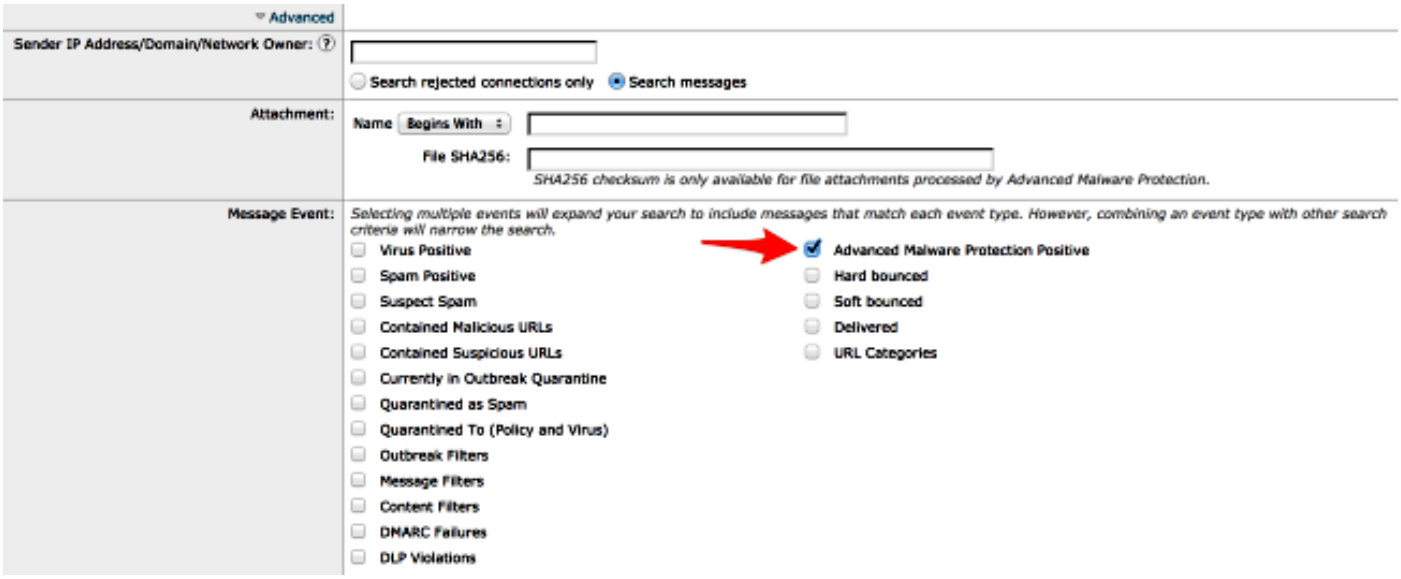
レピュテーション判定は、次に示すように**MALWAREに対**して肯定的です。書き換えられたアクションは、メッセージ変更アクションと[WARNING:**MALWARE DETECTED]** の前に付加されるメッセージ変更アクションと件名行によります。

クリーン ファイルまたは処理中にマルウェアとして特定されなかったファイルの場合は、次の判定がメール ログに書き込まれます。

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

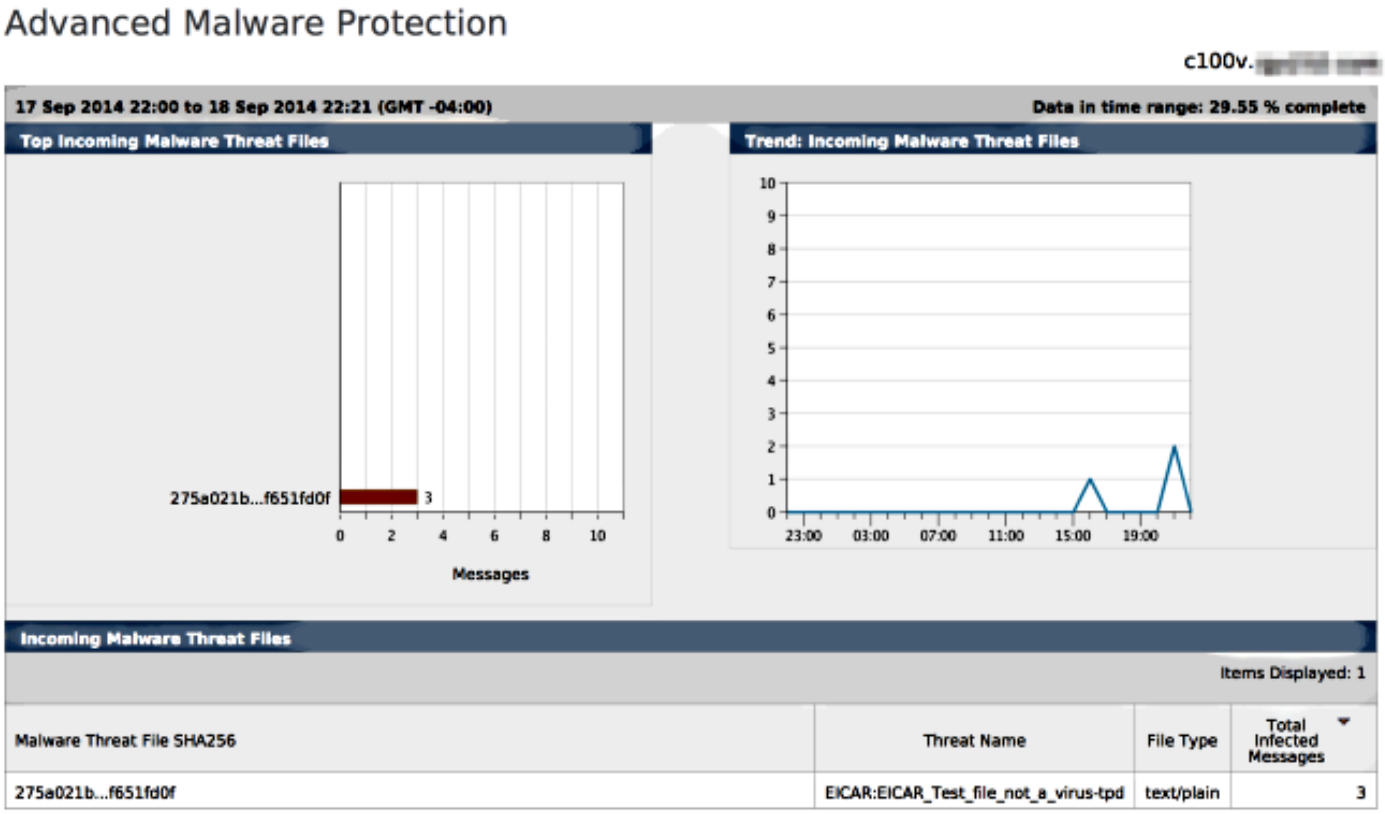
AMP+ メッセージの高度なメッセージ追跡

また、GUI から、メッセージ トラッキングと高度なドロップダウン メニューを使用することによって、高度なマルウェア防御肯定メッセージを直接検索することができます。



高度なマルウェア防御レポート

ESA GUIからは、AMPを介して肯定的に識別されたメッセージのレポートトラッキングも表示されます。[Monitor] > [Advanced Malware Protection]に移動し、必要に応じて時間範囲を変更します。以前の入力の例と同様に表示されます。



トラブルシュート

AMP によって肯定的にスキャンされた既知の本物のマルウェア ファイルが表示されない場合は、メール ログを確認して、AMP がメッセージをスキャンする前に他のサービスがメッセージや

添付ファイルに対してアクションを実行しなかったことを特定します。

以前使用した例で Sophos Anti-virus が有効になっている場合は、それが実際に添付ファイルでウイルスを検出してアクションを実行します。

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
5E71863489DB40@phx.gbl>'
Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final'
Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
<joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine:
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative
Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test'
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus
Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

受信メールポリシーのSophosウイルス対策の構成設定は、ウイルスに感染したメッセージを**ドロップするように設定されています**。この場合、AMPは添付ファイルをスキャンまたは操作するために到達しません。

ただし、いつもそうであるとは限りません。別のサービスまたはコンテンツ/メッセージ フィルタが AMP 処理の前に MID に対するアクションを実行せず、アクションがアクセスされたことを確認するには、メール ログとメッセージ ID (MID) を確認する必要があります。

関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems