ESA高級惡意軟體防護(AMP)測試

目錄

簡介

本文說明如何測試和驗證思科電子郵件安全裝置(ESA)的高級惡意軟體防護(AMP)功能。

在ESA上測試AMP

隨著ESA的AsyncOS 8.5發佈，AMP將執行檔案信譽掃描和檔案分析，以檢測附件中的惡意軟體。

功能鍵

要實施AMP，您必須擁有適用於ESA上的**檔案信譽**和檔案分析**的有效和**活動功能金鑰。請訪問GUI上的**系統管理>功能鍵**，或在CLI上使用**功能鍵**，以驗證功能鍵。

安全服務

若要從GUI啟用該服務，請導航到**Security Services > File Reputation and Analysis**。您可以在CLI中執行**ampconfig**。提交更改並將其提交至配置。

傳入郵件策略

啟用服務後，必須將此服務與傳入郵件策略關聯。

1. 導航到**Mail Policies > Incoming Mail Policies**。
2. 根據需要選擇**預設策略**或預配置的策略。將顯示「傳入郵件策略」頁上的「**高級惡意軟體防護**」列。
3. 選擇列的**Disabled**連結，然後在選項頁上選擇**Enable File Reputation**和**Enable File Analysis**。
4. 您可以根據需要對郵件掃描、不可掃描附件的操作以及已正確識別的郵件執行進一步的配置增強。
5. 提交更改並將其提交至配置。

測試

此時，已啟用您的傳入郵件策略以掃描和檢測惡意軟體。您必須具有用於測試的真實惡意軟體示例。如果您需要有效示例，請訪[問歐洲電腦防病毒研究所(eicar)](#)下載頁面。

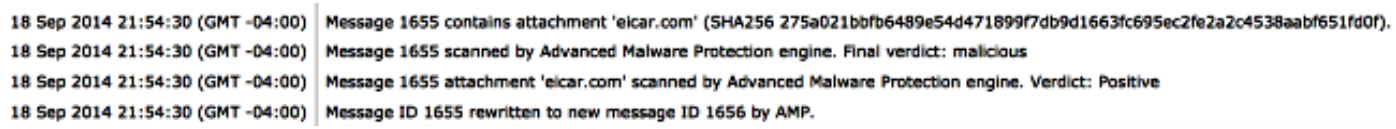
> **注意**：當這些檔案或您的AV掃描器與這些檔案結合使用會對您的電腦或網路環境造成任何損壞時，思科不承擔任何責任。下載這些檔案需要自擔風險。僅當您在使用AV掃描器、電腦設定和網路環境時足夠安全時，才下載這些檔案。提供此資訊是出於測試和複製目的的禮貌。

使用有效的預配置電子郵件帳戶，通過ESA傳送附件並進行正常處理。您可以使用ESA的CLI和**tail mail_logs**來監控郵件處理過程。您將看到郵件日誌中列出的郵件ID(MID)。 螢幕上將顯示類似以下的輸出：

```
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
```

上一個範例顯示，AMP偵測到惡意軟體附件，並根據預設設定，將**dropped**作為最終動作。

從GUI的郵件跟蹤中還可以看到相同的詳細資訊：



如果您選擇從「傳入郵件策略」中傳遞已識別惡意軟體或AMP配置中的其他高級選項，您可能會看到以下郵件處理結果：

```
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
```

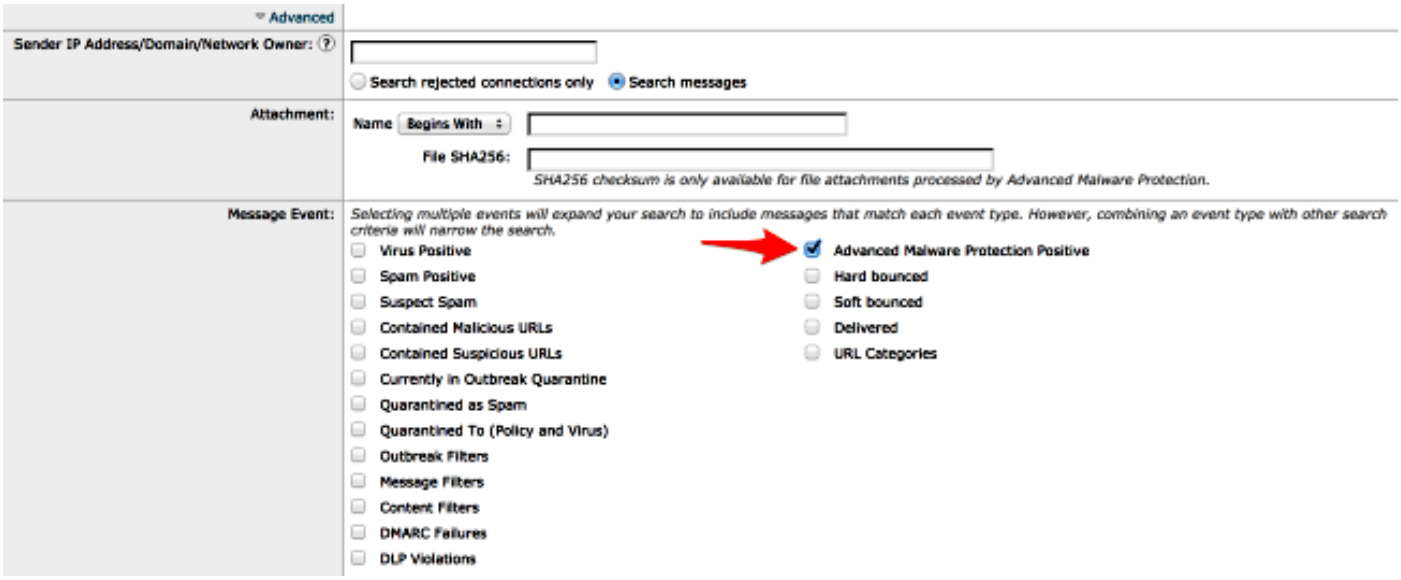
如圖所示，針對**MALWARE**的信譽判定結果仍然為正。重寫操作取決於郵件修改操作和**[警告：檢測到惡意軟體]**。

清除檔案或處理時未識別為惡意軟體的檔案會將此判定寫入郵件日誌：

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

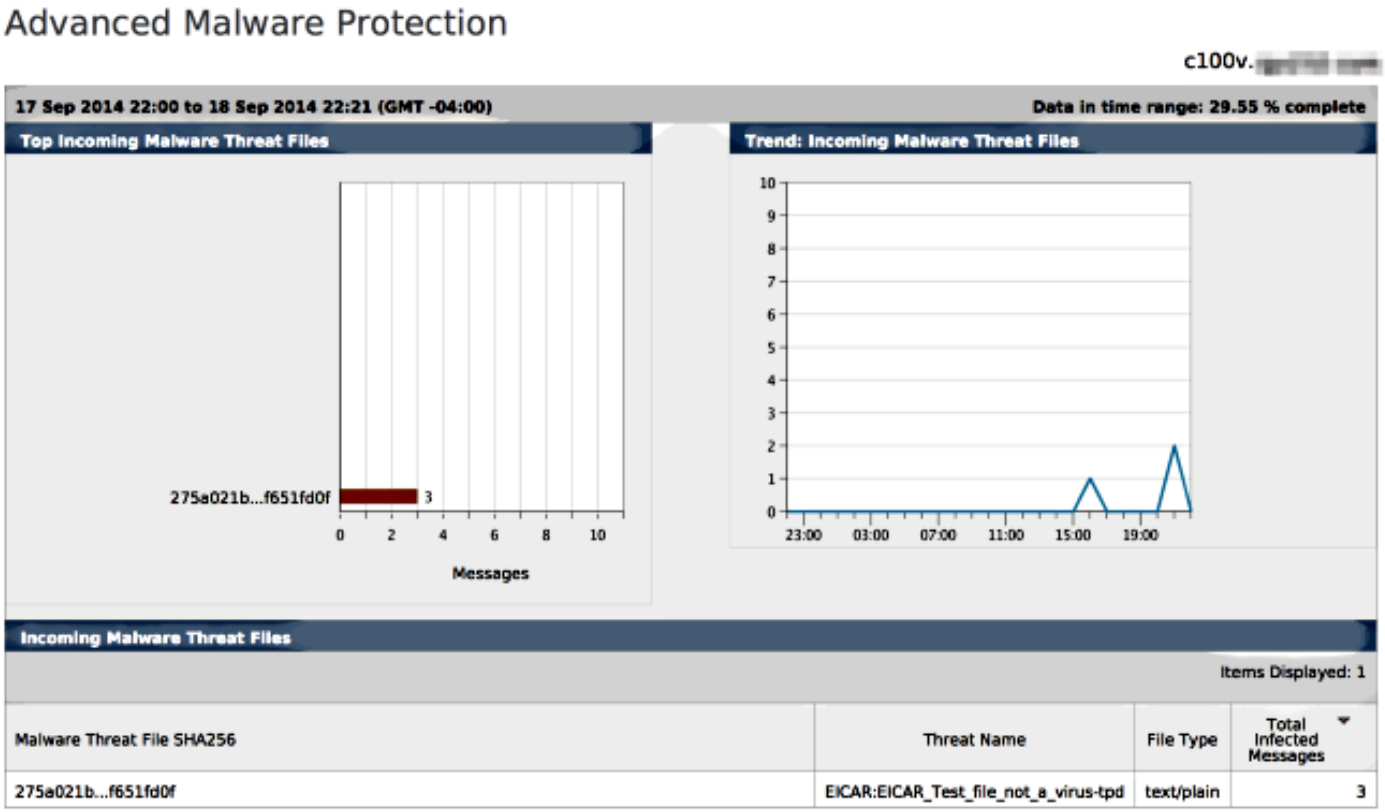
AMP+報文的高級報文跟蹤

此外，在GUI中，使用「郵件跟蹤」(Message Tracking)和「高級」(Advanced)下拉選單時，可以選擇直接搜尋高級惡意軟體防護陽性郵件：



高級惡意軟體防護報告

在ESA GUI中，您還可以通過AMP檢視已正確識別郵件的報告跟蹤。導覽至**Monitor > Advanced Malware Protection**，然後根據需要修改時間範圍。現在您會看到類似內容，前面是輸入示例：



疑難排解

如果您沒有看到已知、真實的AMP正掃描的惡意軟體檔案，請檢視郵件日誌，以確保在AMP掃描郵件之前，其他服務沒有對郵件和/或附件執行操作。

從前面使用的示例來看，啟用Sophos防病毒後，它實際上會捕獲附件並對其執行操作：

```
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
```

傳入郵件策略上的Sophos防病毒配置設定已設定為針對受病毒感染的郵件刪除。在這種情況下，無法訪問AMP以對附件進行掃描或執行操作。

情況並非總是如此。可能需要檢查郵件日誌和郵件ID(MID)，以確保其他服務或內容/郵件過濾器在AMP處理以及達到操作之前未對MID執行操作。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems