檢驗ESA上的檔案分析上傳

目錄

簡介

本文檔介紹如何確定通過思科郵件安全裝置(ESA)上的高級惡意軟體防護(AMP)處理的檔案是否傳送以進行檔案分析，以及關聯的AMP日誌檔案提供什麼。

確定是否上傳附件以進行檔案分析

啟用File Analysis後，File Reputation掃描的附件可能會傳送到File Analysis以進行進一步分析。這提供了針對零日和有針對性的威脅的最高級別的保護。僅當啟用「檔案信譽過濾」時，「檔案分析」才可用。

使用「檔案型別」選項可限制可能傳送到雲的檔案型別。傳送的特定檔案始終基於File Analysis Services Cloud的請求，該請求針對需要進行額外分析的那些檔案。當檔案分析服務雲達到容量時，可能會暫時禁用特定檔案型別的檔案分析。

> **附註**：請參閱適用於思科內容安全產品的高級惡意軟體防護服務的檔案標準思科文檔，瞭解最新資訊和其他資訊。

> **附註**： 有關裝置上運行的AsyncOS的特定版本，請參閱發行說明和使用手冊，因為檔案分析檔案型別可能因AsyncOS的版本而異。

可以傳送用於檔案分析的檔案型別：

- 當前可以傳送以下檔案型別進行分析： （支援檔案分析的所有版本）Windows執行檔，例如.exe、.dll、.sys和.scr檔案。Adobe可移植文檔格式(PDF)、Microsoft Office 2007+(Open XML)、Microsoft Office 97-2004(OLE)、Microsoft Windows/DOS執行檔、其他可能的惡意檔案型別。您選擇上傳到Anti-Malware and Reputation設定頁面（用於Web安全）或File Reputation and Analysis設定頁面（用於Email Security）的檔案型別。 初始支援包括PDF和Microsoft Office檔案。（從AsyncOS 9.7.1 for Email Security開始）如果您已選擇「其他潛在惡意檔案型別」選項，則具有以下副檔名的Microsoft Office檔案將以XML或MHTML格式儲存

：ade，adp，adn，accdb，accdr，accdt，accda，mdb，cdb，mda，mdn，mdt，mdw，mdf，mde，accde，mam，maq，mar，mat，maf，ldb，laccdb，doc，dot，docx，docm，dotx，dotm，dotm，docb，xls，xlt，xlm，xlsx，xlsm，xltx，xltm，xltm，xlsb，xla，xlam，xll，xlw，ppt，pps，pptx，pptm，potx，potx，potx，potx，potx dx、sldm、mht、mhtm、mhtml和xml。

附註：如果「檔案分析」服務的負載超出容量，則即使選擇了檔案型別進行分析，並且檔案在其他情況下符合分析條件，某些檔案也可能無法進行分析。當服務暫時無法處理特定型別的檔案時，您將收到警報。

突出顯示重要附註：

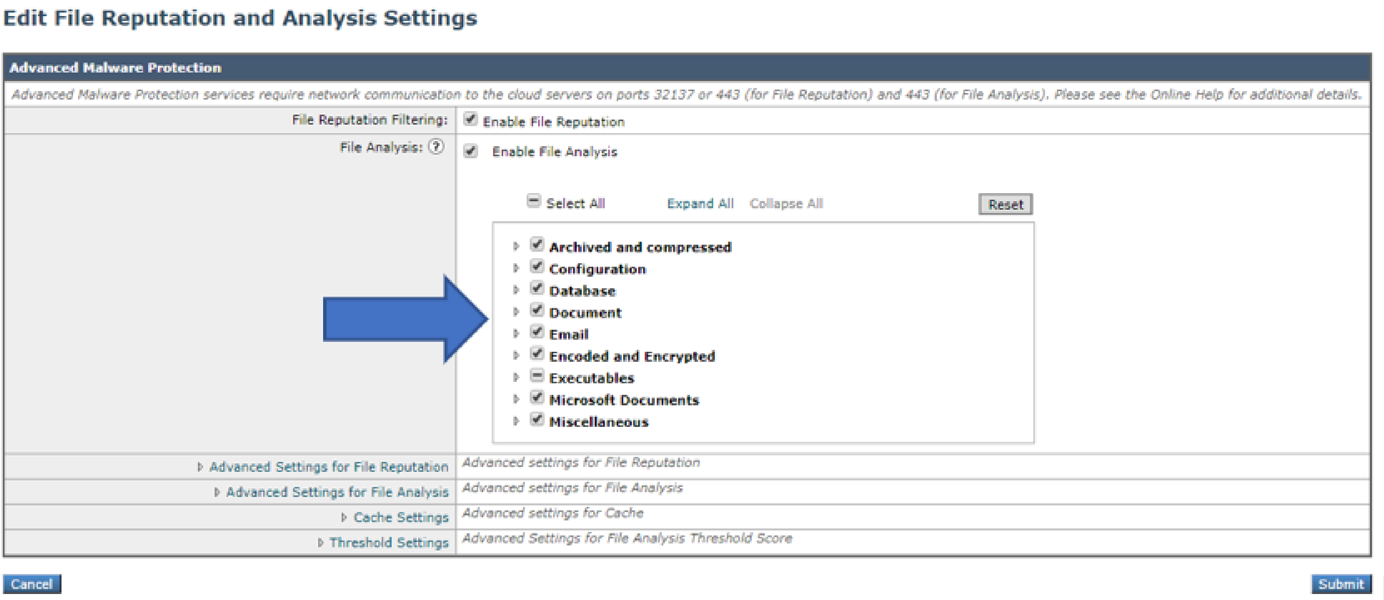
- 如果最近從任何源上載了檔案，則不會再次上載該檔案。有關此檔案的檔案分析結果，請從File Analysis Reporting頁面搜尋SHA-256。
- 裝置將嘗試上傳檔案一次；如果上傳失敗（例如由於連線問題），則可能無法上傳檔案。如果由於檔案分析伺服器超載而失敗，將再次嘗試上載。

配置用於檔案分析的AMP

預設情況下，當ESA首次開啟且尚未與Cisco更新程式建立連線時，列出的唯一檔案分析檔案型別將是「Microsoft Windows/DOS執行檔」。 在允許配置其他檔案型別之前，您需要允許完成服務更新。 這將反映在updater_logs日誌檔案中，該檔案被視為「fireamp.json」：

```
Sun Jul 9 13:52:28 2017 Info: amp beginning download of remote file
"http://updates.ironport.com/amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp successfully downloaded file
"amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp applying file "amp/1.0.11/fireamp.json/default/100116"
```

要通過GUI配置檔案分析，請導航到**安全服務>檔案信譽和分析>編輯全域性設定......**


Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering: ☑ Enable File Reputation

File Analysis: ☑ Enable File Analysis

⊟ Select All

- ☑ Archived and compressed
- ☑ Configuration
- ☑ Database
- ☑ Document
- ☑ Email
- ☑ Encoded and Encrypted
- ⊟ Executables
- ☑ Microsoft Documents
- ☑ Miscellaneous

Advanced Settings for File Reputation: Advanced settings for File Reputation

Advanced Settings for File Analysis: Advanced settings for File Analysis

Cache Settings: Advanced settings for Cache

Threshold Settings: Advanced Settings for File Analysis Threshold Score

要通過CLI配置用於檔案分析的AMP，請輸入**ampconfig > setup**命令並瀏覽響應嚮導。如果出現以下問題，則必須選擇Y:**是否要修改檔案分析的檔案型別？**

```
myesa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> setup

File Reputation: Enabled
Would you like to use File Reputation? [Y]>

Would you like to use File Analysis? [Y]>

File types supported for File Analysis:

1. Archived and compressed [selected]
2. Configuration [selected]
3. Database [selected]
4. Document [selected]
5. Email [selected]
6. Encoded and Encrypted [selected]
7. Executables [partly selected]
8. Microsoft Documents [selected]
9. Miscellaneous [selected]

Do you want to modify the file types selected for File Analysis? [N]> y

Enter comma separated serial numbers from the "Supported" list. Enter "ALL" to select all
"currently" supported File Types.
[1,2,3,4,5]> ALL

Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy.
```

根據此配置，啟用的檔案型別受檔案分析（如果適用）的制約。

檢視AMP日誌進行檔案分析

當附件由ESA上的檔案信譽或檔案分析掃描時，它們會記錄在AMP日誌中。若要檢視所有AMP操作的此日誌，請從ESA的CLI運行**tail amp**，或遍歷**tail**或**grep**命令的響應嚮導。如果您知道要在AMP日誌中搜尋的特定檔案或其他詳細資訊，**grep**命令非常有用。

以下是範例：

```
mylocal.esa >  tail amp

Press Ctrl-C to stop.
Tue Aug 13 17:28:47 2019 Info: Compressed/Archive File: sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac MID = 1683600, Extracted File: File Name =
'[redacted].pdf', File Type = 'application/pdf', sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac, Disposition = LOWRISK, Response received from =
Cloud, Malware = None, Analysis Score = 0, upload_action = Recommended to send the file for
analysis
Thu Aug 15 13:49:14 2019 Debug: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Thu Aug 15 13:49:14 2019 Debug: Response received for file reputation query from Cloud. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

附註：較舊版本的AsyncOS將在AMP日誌中顯示「amp_watchdog.txt」。 這是一個在日誌中每十分鐘顯示一次的OS檔案。此檔案是AMP的keep-alive的一部分，可以安全忽略。 此檔案從AsyncOS 10.0.1及更新版本開始隱藏。

附註：較舊版本的AsyncOS將記錄upload_action標籤，該標籤具有三個為上載到檔案分析行為定義的值。

在舊版AsyncOS上執行上載操作的三個響應：

- "upload_action = 0":信譽服務知道該檔案；不傳送進行分析。
- "upload_action = 1":傳送
- "upload_action = 2":信譽服務知道該檔案；不傳送進行分析

在AsyncOS版本12.x及更高版本上執行上載操作的兩個響應：

- "upload_action =建議傳送檔案進行分析"
- **僅調試日誌**:"upload_action =建議不要傳送檔案進行分析"

此響應指示是否傳送檔案進行分析。同樣，它必須符合配置檔案型別的標準，才能成功提交。

上載操作標籤說明

```
"upload_action = 0": The file is known to the reputation service; do not send for analysis.
```

對於「0」，這意味著檔案「不需要傳送以進行上傳」。 或者，檢視此檔案的更好方法是如果需要，*可*將檔案傳送至File Analysis*上傳*。 但是，如果檔案不*必需*，則不會傳送該檔案。

```
"upload_action = 2": The file is known to the reputation service; do not send for analysis
```

對於「2」，這是嚴格的「不傳送」上傳檔案。 此操作是最終且決定性的，並且檔案分析處理已完成。

範例案例

本節介紹一些可能的情況，在這些情況下，檔案或是正確上傳以進行分析，或是由於特定原因而未上傳。

已上載檔案進行分析

舊版AsyncOS:

此範例顯示符合條件且使用**upload_action = 1**標籤的DOCX檔案。在下一行中，**File uploaded for analysis** Secure Hash Algorithm(SHA)也會記錄到AMP記錄中。

```
Thu Jan 29 08:32:18 2015 Info: File reputation query initiating. File Name = 'Lab_Guide.docx',
MID = 860, File Size = 39136 bytes, File Type = application/msword
Thu Jan 29 08:32:19 2015 Info: Response received for file reputation query from Cloud. File Name
= 'Royale_Raman_Lab_Setup_Guide_Beta.docx', MID = 860, Disposition = file unknown, Malware =
None, Reputation Score = 0, sha256 =
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce, upload_action = 1
Thu Jan 29 08:32:21 2015 Info: File uploaded for analysis. SHA256:
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce
```

AsyncOS 12.x及更高版本：

此範例顯示符合條件且使用**upload_action = Recommended標籤的PPTX檔案以傳送檔案進行分析**。在下一行中，上傳的**檔案用於分**析安全雜湊演算法(SHA)也會記錄到AMP日誌中。

```
Thu Aug 15 09:42:19 2019 Info: Response received for file reputation query from Cloud. File Name
= 'ESA_AMP.pptx', MID = 1763042, Disposition = UNSCANNABLE, Malware = None, Analysis Score = 0,
sha256 = 0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, upload_action = Recommended to
send the file for analysis
Thu Aug 15 10:05:35 2019 Info: File uploaded for analysis. SHA256:
0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, file name: ESA_AMP.pptx
```

未上載檔案進行分析，因為檔案已知

舊版AsyncOS:

此示例顯示AMP掃描的PDF檔案，該檔案信譽日誌附加了**upload_action = 2**。此檔案對於雲已知，不需要上載以進行分析，因此不會再次上載。

```
Wed Jan 28 09:09:51 2015 Info: File reputation query initiating. File Name = 'Zombies.pdf', MID
= 856, File Size = 309500 bytes, File Type = application/pdf
Wed Jan 28 09:09:51 2015 Info: Response received for file reputation query from Cache. File Name
= 'Zombies.pdf', MID = 856, Disposition = malicious, Malware = W32.Zombies.NotAVirus, Reputation
Score = 7, sha256 = 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002,
upload_action = 2
```

AsyncOS 12.x及更高版本：

此範例顯示amp_watchdog.txt檔案，其中偵錯層級的amp記錄與**upload_action =建議不要將檔案傳送到檔案信譽記錄後進行分**析。此檔案對於雲已知，不需要上載以進行分析，因此不會再次上載。

```
Mon Jul 15 17:41:53 2019 Debug: Response received for file reputation query from Cache. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

記錄檔案分析通過郵件標頭上傳

在CLI中，通過使用**logconfig**命令的選項，可以選擇**logheaders**子選項來列出和記錄通過ESA處理的

電子郵件的標頭。使用「X-Amp-File-Uploaded」標頭，無論何時上傳或未上傳檔案以進行檔案分析，檔案都將記錄到ESA的郵件日誌中。

檢視郵件日誌，檢視上載的檔案進行分析的結果：

```
Mon Sep 5 13:30:03 2016 Info: Message done DCID 0 MID 7659 to RID [0] [('X-Amp-File-Uploaded',
'True')]
```

檢視郵件日誌，檢視未上載的檔案進行分析的結果：

```
Mon Sep 5 13:31:13 2016 Info: Message done DCID 0 MID 7660 to RID [0] [('X-Amp-File-Uploaded',
'False')]
```

相關資訊

- AsyncOS使用手冊
- 適用於思科內容安全產品的高級惡意軟體防護服務的檔案標準
- ESA高級惡意軟體防護(AMP)測試
- 技術支援與文件 - Cisco Systems