ESA のファイル 分析アップロードの検証

目次

概要

この資料に AMP 関連するログファイルが提供する何を Cisco E メール セキュリティ アプライアンス（ESA）の Advanced Malware Protection （AMP）によって処理されるファイルがファイル分析のために送信 される、およびまたかどうか判別する方法を記述されています。

添付ファイルがファイル 分析のためにアップロードされたかどうか確認して下さい

ファイルによって分析は、更なる分析のためのファイル 分析にファイル評判によって送信 されるかもしれないスキャンされる添付ファイル有効に なります。 これはゼロ日のおよび目標とされた脅威に対して保護の最高レベルを提供します。 ファイル 分析はファイル評判フィルタリングが有効に なるときだけ利用できます。

Cloud に送信 されるかもしれないファイルの種類を制限するためにファイルタイプ オプションを使用して下さい。 送信 される特定のファイルはファイル 分析 サービス Cloud からの要求に常に基づいています、追加分析が必要であるそれらのファイルを目標とする。 特定のファイル型のためのファイル 分析はファイル 分析 サービス Cloud がキャパシティに達する一時的に無効に なるかもしれません。

> **注:** 最新およびその他の情報に関しては Cisco コンテンツ セキュリティ製品 Ciscoドキュメントの Advanced Malware Protection サービスのためのファイル 基準を参照して下さい。

> **注:** ファイル 分析 ファイルタイプが AsyncOS のバージョンに基づいて変わるかもしれないので、アプライアンスで動作する AsyncOS の特定の修正のためのリリース ノートおよびユーザガイドを検討して下さい。

ファイル 分析のために送信 することができるファイルタイプ:

- 次のファイルタイプは分析のために現在 送信 することができます:（すべてのリリース ファ

イル 分析をサポートする ） Windows 実行、たとえば .exe、.dll、.sys および .scr ファイル。 Adobe Portable document format （ PDF ）、Microsoft Office 2007+ （ 開いた XML ）、Microsoft Office 97-2004 （ OLE ）、Microsoft Windows/DOS 実行可能モジュール、他の可能性としては悪意のあるファイルタイプ。Settings ページ反Malware のアップ ロードにおよび評判 (Web セキュリティのために) または Settings ページ ファイル評判および分析選択したファイルタイプ (E メール セキュリティのために。 ） 最初のサポートは PDF および Microsoft Office ファイルが含まれています。他の可能性としては悪意のあるファイルタイプオプションを選択する場合 (E メール セキュリティ用の AsyncOS 9.7.1 の始まり) 、次の拡張機能が付いている Microsoft Office ファイルは XML または MHTML 形式で保存しました: ade、adp、adn、accdb、accdr、accdt、accda、mdb、cdb、mda、MDN、mdt、mdw、mdf、mde、accde、mam、maq、3 月、マット、maf、ldb、laccdb、ドキュメント、ドット、docx、docm、dotx、dotm、docb、xls、xlt、xlm、xlsx、xlsm、xltx、xltm、xlsb、xla、xlam、xll、xlw、ppt、pot、pps、pptx、pptm、potx、potm、ppam、ppsx、ppsm、sldx、sldm、mht、mhtm、mhtml および XML。

注: ファイル 分析サービスのロードがキャパシティを超過する場合、いくつかのファイルはファイルタイプが分析に選択され、もファイルが他では分析のために適格である分析されないかもしれません。 サービスが一時的に特定の種類のファイルを処理することができないときアラートを受け取ります。

注記の強調表示:

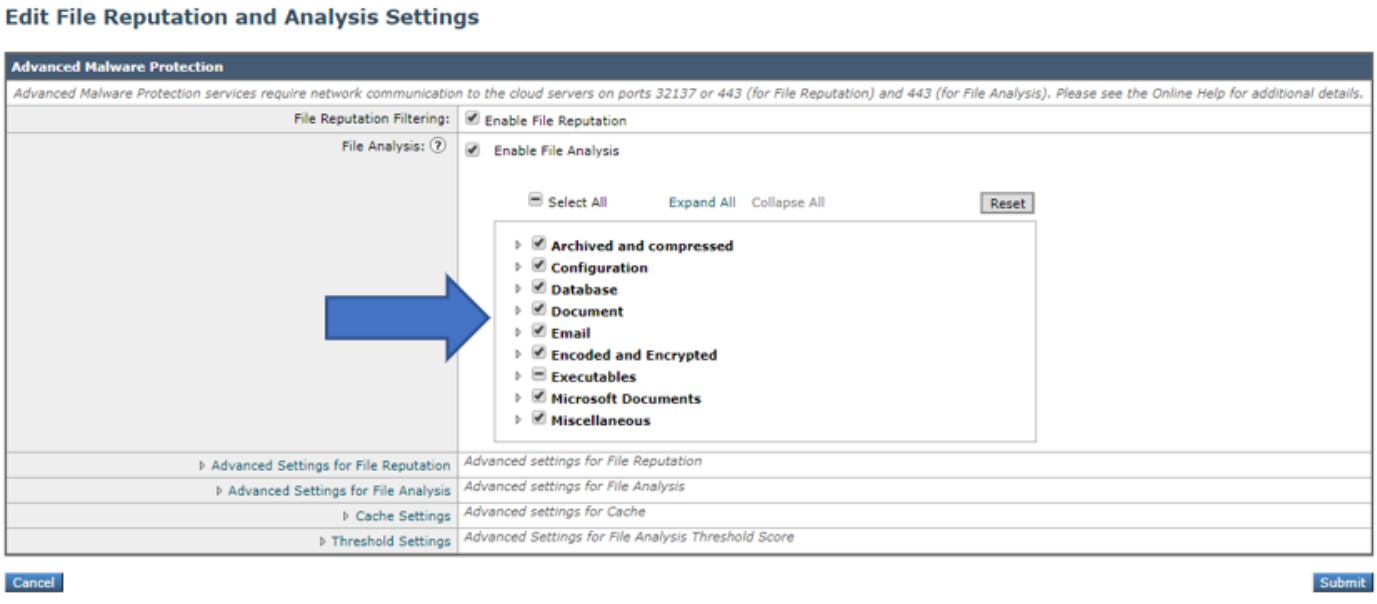
- ファイルがあらゆる出典から最近アップロードされる場合、ファイルは再度アップロードされません。 このファイルのファイル 分析結果に関しては、ページを報告するファイル 分析からの SHA-256 のための検索。
- アプライアンスはファイルをアップロードすることを一度試みます; アップロードが正常ではない場合、たとえば接続に関する問題が理由で、ファイルはアップロードされないかもしれません。 ファイル 分析 サーバが過剰になったので失敗があったら、アップロードはもう一度試みられます。

ファイル 分析のための設定 AMP

デフォルトで ESA が最初に起動され、まだ Cisco アップデータへの接続を確立するために持っている場合、リストされている唯一のファイル 分析 ファイルタイプは「Microsoft Windows/DOS 実行可能モジュール」ファイルです。 サービス アップデートが追加ファイルタイプを設定することができる前に完了するように必要があります。 これは「fireamp.json として」見られた updater_logs 口グファイルに反映されます:

```
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"
```

ファイル 分析を**セキュリティ サービス > ファイル評判および分析 > Edit グローバルな設定**に GUI、ナビゲートによって設定するため...



ファイル 分析のための AMP を CLI によって設定するために、応答ウィザードを通して **ampconfig > setup コマンド**および移動を入力して下さい。 この質問が表示されるとき『Y』 を選択 して下さい: **ファイル 分析に対するファイルタイプを修正したいと思いますか。**

```
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.
```

この設定に基づいて、有効に なる ファイルタイプは適当ようにファイル 分析に応じて、あります。

ファイル 分析のための確認 AMP ログ

添付ファイルが ESA のファイル評判かファイル 分析によってスキャンされるとき、AMP ログに記録されます。 AMP すべてのアクションのためのこの口グを見るために、**tail amp を** ESA の CLI から実行するか、またはどちらかのための応答ウィザードを通して **tail または grep コマンドを**移動して下さい。 **grep コマンドは** AMP ログで捜すことを望む他の詳細か特定のファイルを知っている場合役立ちます。

次に例を示します。

```
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
```

> **注:** AsyncOS のより古いバージョンは AMP ログの「amp_watchdog.txt」を表示する。 10 分毎に口グの表示するこれは OS ファイルです。 このファイルは AMP のためのキープアライブの一部で、安全に無視されるかもしれません。 このファイルは AsyncOS 10.0.1 の隠された開始およびより新しいです。

> **注:** ファイル 分析 動作へのアップロードのために定義される AsyncOS のより古いバージョンは upload_action タグを持っています 3 つの値を記録 します。

より古い AsyncOS のアップロード操作のための 3 つの応答:

- 「upload_action = 0": ファイルは評判サービスに知られています; 分析のために送信 しないで下さい。

- 「upload_action = 1": 送信
- 「upload_action = 2": ファイルは評判サービスに知られています; 分析のために送信 しないで下さい

のおよび前のアップ ロード アクション AsyncOS バージョン 12.x のための 2 つの応答:

- 「upload_action = 分析のためのファイルを」送信 することを推奨される
- **デバッグはただ記録 します:**「upload_action = 分析のためのファイルを」は送信 しないことを推奨しました

この応答はファイルが分析のために送信 されるかどうか定めます。 再度、それは設定されたファイルタイプの条件を正常に入るために満たす必要があります。

アップロード処理タグの説明

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`
"0," のためにこれはファイルが「アップロードのために」送信 されるために必要とされないことを意味します。 または、それを検知 するよりよい方法はファイル 分析にアップロードのために、ファイル*必要であれば*送信 することができますあります。 ただし、ファイルがそれから必要とならなければファイルは送信 されません。

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`
これによってが厳密「である "2," のために」アップロードのためのファイルを送信 しない で下さい。 この操作は最終的、決定的であり、ファイル 分析処理は実行されます。

シナリオ例

このセクションはファイルが分析のためにきちんとアップロードされるか、または特定の原因がアップロードされなかった原因ではない可能なシナリオを解説しています。

分析のためにアップロードされるファイル

より古い AsyncOS:

条件を満たし、**upload_action と = 1.**タグ付けされるこの例は DOCX ファイルを表示したものです。 次の行では、**分析** Secure Hash Algorithm (SHA) **のためにアップロードされるファイルは** AMP ログに同様に記録されます。

```
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 および前に:

条件を満たし、**upload_action と = 分析のためのファイルを送信 することを推奨されて**タグ付けされるこの例は PPTX ファイルを表示したものです。 次の行では、**分析** Secure Hash Algorithm (SHA) **のためにアップロードされるファイルは** AMP ログに同様に記録されます。

```
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
```

ファイルが既に知られているので分析のためにアップロードされないファイル

より古い AsyncOS:

upload_action の AMP によって = ファイル評判ログに追加 される 2 スキャンされるこの例は PDFファイルを示したものです。 Cloud にこのファイルがまだ知られ、分析のためにアップロードされるために必要となっていません従って再度アップロードされません。

```
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 および前に:

この例はアンペアの amp_watchdog.txt ファイルが upload_action と一致するデバッグ レベルを = ファイル評判ログに追加 される **分析のためのファイルを送信 しないことを推奨されて**ログオンすることを示します。 Cloud にこのファイルがまだ知られ、分析のためにアップロードされるために必要となっていません従って再度アップロードされません。

```
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
```

メール ヘッダによるロギング ファイル 分析アップロード

コマンド logconfig を使用してオプションの CLI から、ESA によって処理されるメールのヘッダをリストし、記録 するために、logheaders のサブ オプションは選択することができます。 を使用するファイルがアップロードされるか、またはファイル 分析のためにアップロードされなくて ESA のメール ログに記録される、ヘッダを「X AMP ファイル アップロードしました」。

メールを検知 して 分析のためにアップロードされるファイルのために記録 しましたり、起因します:

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

メールを検知 して 分析のためにアップロードされないファイルのために記録 しましたり、起因します:

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

関連情報

- AsyncOS ユーザ ガイド
- Cisco コンテンツ セキュリティ製品の Advanced Malware Protection サービスのためのファイル 基準
- ESA の Advanced Malware Protection (AMP) のテスト
- テクニカル サポートとドキュメント – Cisco Systems