

ESA のファイル 分析アップロードの検証

目次

[概要](#)

[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 分析のための AMP を設定して下さい](#)

[ファイル 分析のための AMP ログを見て下さい](#)

[アップロード処理 "2" vs アップロード処理 "0" の説明](#)

[シナリオ例](#)

[分析のためにアップロードされるファイル](#)

[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](#)

[電子メール ヘッダによるロギング ファイル 分析アップロード](#)

[関連情報](#)

概要

この資料に関連する AMP 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断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ディセーブルにされるかもしれません。

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)、次の拡張を用いる 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、マツト、maf、ldb、laccdb、ドキュメント、ドット、docx、docm、dotx、dotm、docb、xls、xlt、xlm、xlsx、xlsm、xltx、xltn、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 ロ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...

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:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: ?	<input checked="" type="checkbox"/> Enable File Analysis
	File Types: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Adobe Portable Document Format (PDF) <input checked="" type="checkbox"/> Microsoft Office 2007+ (Open XML) <input checked="" type="checkbox"/> Microsoft Office 97-2004 (OLE) <input checked="" type="checkbox"/> Microsoft Windows / DOS Executable
Advanced Settings for File Reputation	Cloud Domain: <input type="text" value="a.immunet.com"/>
	Cloud Server Pool: <input type="text" value="cloud-sa.amp.sourcefire.com"/>
	SSL Communication for File Reputation: <input checked="" type="checkbox"/> Use SSL (Port 443)
	Tunnel Proxy (Optional): <ul style="list-style-type: none"> Server: <input type="text"/> Port: <input type="text"/> Username: <input type="text"/> Password: <input type="password"/> Retype Password: <input type="password"/> <input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy ?
	Heartbeat Interval: <input type="text" value="15"/> minutes
	Reputation Threshold: <ul style="list-style-type: none"> <input checked="" type="radio"/> Use Value from Cloud Service (60) <input type="radio"/> Enter Custom Value: <input type="text" value="60"/> <ul style="list-style-type: none"> (Valid range 1 through 100)
	Query Timeout: <input type="text" value="15"/> seconds
	Processing Timeout: <input type="text" value="120"/> seconds
	File Reputation Client ID: <input type="text" value=""/>
	File Analysis Server URL: <input type="text" value="AMERICAS (https://panacea.threatgrid.com)"/>
	File Analysis Client ID: <input type="text" value="01_VLNESA..._C100V_00000000"/>

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 **amponfig > 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せんか。**

```
myesa.local> amponfig
```

```
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. Adobe Portable Document Format (PDF) [selected]
2. Microsoft Office 2007+ (Open XML) [selected]
3. Microsoft Office 97-2004 (OLE) [selected]
4. Microsoft Windows / DOS Executable [selected]
5. Other potentially malicious file types [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、ありません。

ファイル分析のための確認 AMP ログ

添付ファイルが ESA のファイル評判が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。すべての AMP アクションのためのこのログを見るために、**テールアンペア**を ESA の CLI から実行するか、または**テール**または **grep** コマンドのための応答ウィザードを通して移動して下さい。**grep** コマンドは AMP ログで探すことを望む他の詳細が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。

```
myesa.local> tail amp
```

Press Ctrl-C to stop.

```
Mon Feb 2 14:45:35 2015 Info: File reputation query initiating. File Name = 'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 14:45:35 2015 Info: Response received for file reputation query from Cache. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcd403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
Mon Feb 2 14:55:35 2015 Info: File reputation query initiating. File Name = 'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 14:55:35 2015 Info: Response received for file reputation query from Cache. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcd403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
Mon Feb 2 15:05:35 2015 Info: File reputation query initiating. File Name = 'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 15:05:35 2015 Info: Response received for file reputation query from Cache. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcd403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

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分毎にロ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。

評判のために処理されてファイルがファイル評判クエリの終わりにタグ付けされるそれらに **upload_action** があります。アップロード操作のための 3 つの応答があります:

- 「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

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 "2" vs アップロード処理 "0" 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。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

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、分析セキュアハッシュアルゴリズム (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
```

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

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
```

電子メール 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電子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](#)