在ESA的正在验证的文件分析加载

目录

简介

本文描述如何确定通过先进的恶意软件保护的文件(安培)处理在思科电子邮件安全工具(ESA)是否为文件分析发送，并且什么相关的安培日志文件提供。

确定附件是否为文件分析上传

使用文件分析启用，由文件名誉扫描可能发送到进一步分析的文件分析的附件。这提供最高水平保护零天和被瞄准的威胁。当文件名誉过滤启用时，文件分析只是可用的。

请使用文件类型选项为了限制也许发送到Cloud文件的种类。发送的特定文件根据从文件分析服务Cloud的请求总是，瞄准那些文件另外的分析是需要的。当文件分析服务Cloud到达产能时，特定的文件类型的文件分析也许临时地禁用。

> **注意**：参考先进的恶意软件保护业务的文件标准思科内容安全产品Cisco文档的最最新和其他信息。

> **注意**： 请查看版本注释和用户指南在您的设备运行AsyncOS的特定版本的，因为文件分析文件类型可能变化基于AsyncOS版本。

可以为文件分析发送的文件类型：

- 以下文件类型可能为分析当前发送： (支持文件分析)的所有版本Windows可执行软件，例如.exe、.dll、.sys和.scr文件。Adobe便携式文件格式(PDF)，微软办公软件2007+ (开放XML)，微软办公软件97-2004 (OLE)， Microsoft Windows/DOS可执行，其他潜在有恶意的文件类型。您为在Settings页的反恶意软件的加载选择和的名誉的文件类型(Web安全)或Settings页文件的名誉和的分析(电子邮件安全。)初始支持包含PDF和微软办公软件文件。(开始处在电子邮件安全的AsyncOS 9.7.1)，如果选择另一个潜在有恶意的文件类型选项，有在XML或MHTML格式保存的以下扩展的微软办公软件文件：ade、adp、adn、accdb、accdr、accdt、accda、mdb、cdb、mda、mdn、mdt、mdw、mdf、mde、accde、mam、maq、3月

、席子、maf、ldb、laccdb、文档、小点、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和xml。

注意：如果在文件分析服务的负载超出产能，不可以分析一些文件，即使文件类型为分析选择，并且文件否则有资格分析。当服务临时地无法处理特定类型的文件，您将收到警报。

突出显示重要提示：

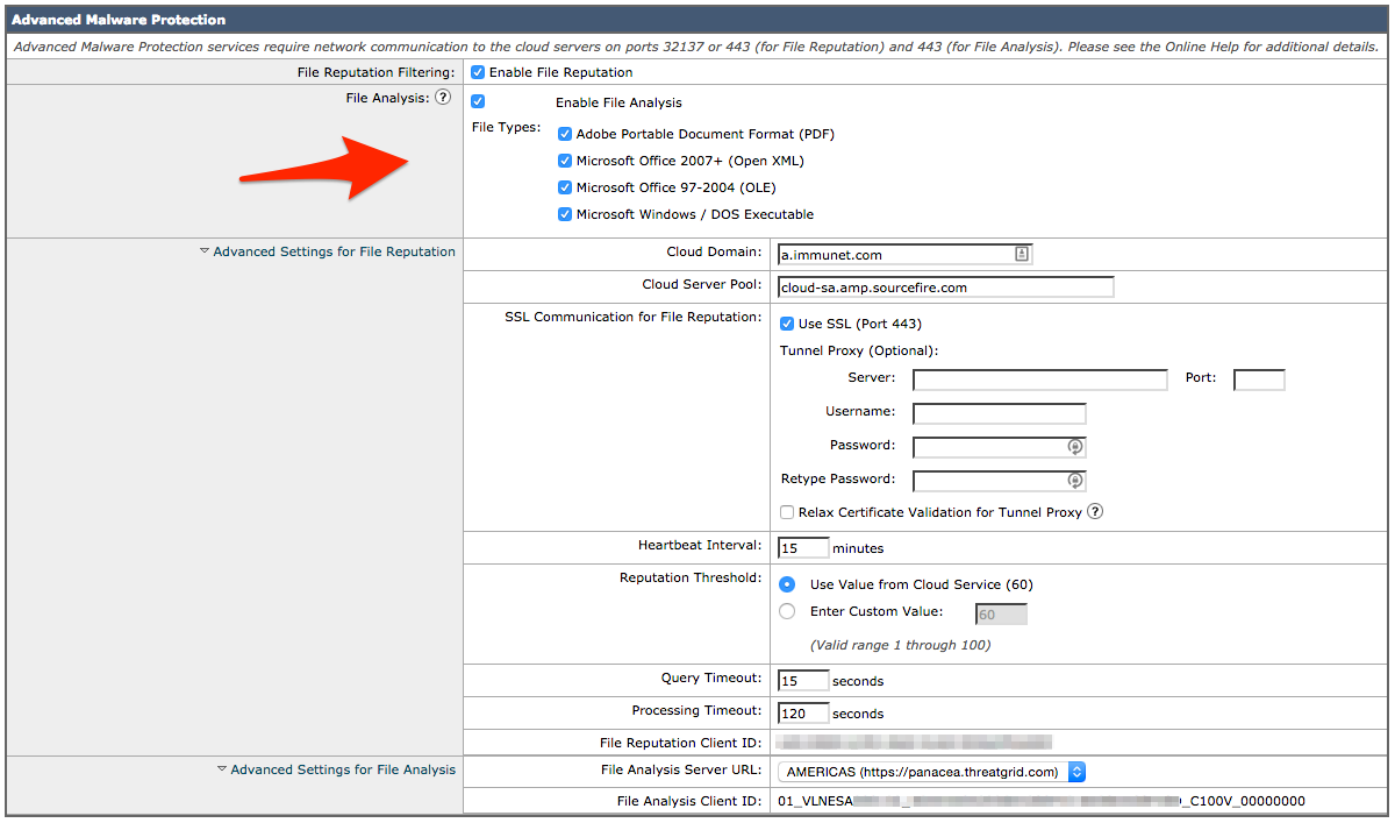
- 如果文件从任何来源最近上传，文件不会再上传。文件此文件的分析结果， SHA-256的搜索从报告页的文件分析。
- 设备一次将设法上传文件;如果加载不是成功的，例如由于连接问题，文件不可以上传。如果失败是，因为超载了文件分析服务器，加载更加将尝试。

配置文件分析的安培

默认情况下，当ESA首先打开并且有建立对思科更新的连接，列出的唯一的文件分析文件类型将是“Microsoft Windows/DOS可执行”文件。 您将需要允许服务更新在配置之前其它文献类型的允许完成。 这在updater_logs日志文件将反射，被看到作为“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"
```

通过GUI要配置文件分析，请导航对**安全服务>文件名誉和分析> Edit全局设置...**



为了通过CLI配置文件分析的安培，请输入**ampconfig > setup命令**并且通过答复向导移动。当您提交与此问题时，您必须选择**Y** ： **是否要修改文件分析的文件类型？**

```
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. 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.
```

凭此配置，启用的文件类型是受文件分析支配，如可适用。

复核文件分析的安培日志

当附件由文件名誉或文件分析扫描在ESA时，他们在安培日志被记录。为了检查所有安培操作的此日志，从ESA的CLI请运行**尾标安培**或者通过或者**尾标的**答复向导移动或**grep命令**。 **grep命令**是有用的，如果认识您在安培日志希望搜索的特定文件或其他详细信息。

示例如下：

```
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 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, 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 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, 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 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

> **注意**：AsyncOS更旧的版本将显示“amp_watchdog.txt”在安培日志。 显示在日志的每十分钟的这是操作系统文件。此文件是一部分的keep-alive安培的，并且可能安全忽略。 此文件是隐藏的开始在AsyncOS 10.0.1和更新。

使用为名誉处理的文件，他们有**upload_action**被标记在文件名誉查询结束时。有加载操作的三答复：

- “upload_action = 0" ：文件为名誉服务所知;请勿为分析发送。
- “upload_action = 1" ：发送
- “upload_action = 2" ：文件为名誉服务所知;请勿为分析发送

此答复指明文件是否为分析发送。再次，它必须满足已配置的文件类型的标准为了顺利地提交。

加载操作"0"的说明与加载操作"2"

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

对于"0,"这意味着文件“没有必要为加载发送”。或者，一个更加好的方式查看它是，文件*可以*为加载*如果必须*发送到文件分析。 然而，如果文件然后没有要求文件没有发送。

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

对于"2,"这的严格“请勿发送”加载的文件。 此操作最终和果断，并且文件分析处理完成。

示例情景

此部分描述文件为分析适当地上传或不上传的归结于一个特定原因的可能的情况。

为分析上传的文件

此示例显示满足标准和用**upload_action**标记**= 1.的**DOCX文件**。**在下一条，**为分析**安全哈希算法(SHA)**上传的文件**被记录对安培日志。

```
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
```

为分析没上传的文件，由于文件已经知道

由与**upload_action的**安培扫描**= 2**被添附对文件名誉日志的此示例显示PDF文件。此文件已经为Cloud所知和没有要求为分析上传，因此再没有上传。

```
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
```

日志文件分析加载通过电子邮件报头

从CLI，与选项使用命令**logconfig**， **logheaders的**子选项可以选择列出和记录通过ESA处理的电子邮件报头。 使用“X安培FILE上传”报头，文件上传或没上传为文件分析将被记录对ESA的邮件日志。

查看邮件日志，结果为上传的文件为分析：

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

查看邮件日志，结果为没上传的文件为分析：

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

相关信息

- AsyncOS用户指南
- 先进的恶意软件保护业务的文件标准思科内容安全产品的
- ESA提前的恶意软件保护(安培)测验
- 技术支持和文档 - Cisco Systems