التحقق من تحميلات تحليل الملفات على ESA

المحتويات

المقدمة

يوضح هذا المستند كيفية تحديد ما إذا كانت الملفات التي تتم معالجتها من خلال الحماية المتقدمة من البرامج الضارة (AMP) على جهاز أمان البريد الإلكتروني من Cisco (ESA) يتم إرسالها لتحليل الملفات، وكذلك ما يقدمه ملف سجل AMP المقترن.

تحديد ما إذا كان قد تم تحميل المرفقات لتحليل الملف أم لا

مع تمكين تحليل الملفات، قد يتم إرسال المرفقات التي تم مسحها ضوئيا بواسطة "سمعة الملف" إلى "تحليل الملفات" لمزيد من التحليل. يوفر ذلك أعلى مستوى من الحماية ضد التهديدات المستهدفة والتي تكون في يوم صفر. يتوفر تحليل الملف فقط عند تمكين تصفية سمعة الملف.

أستخدم خيارات أنواع الملفات لتحديد أنواع الملفات التي قد يتم إرسالها إلى مجموعة النظراء. تستند الملفات المحددة التي يتم إرسالها دائما إلى الطلبات الواردة من مجموعة "خدمات تحليل الملفات"، والتي تستهدف هذه الملفات التي يلزم إجراء تحليل إضافي لها. قد يتم تعطيل تحليل الملفات لأنواع ملفات معينة بشكل مؤقت عندما تصل سحابة خدمات تحليل الملفات إلى السعة.

ملاحظة: ارجع إلى معايير الملف لخدمات الحماية المتقدمة من البرامج الضارة لمنتجات أمان المحتوى من Cisco مستند Cisco للحصول على أحدث المعلومات والمعلومات الإضافية.

ملاحظة: الرجاء مراجعة ملاحظات الإصدار ودليل المستخدم لإجراء مراجعة محددة لنظام التشغيل AsyncOS الذي يتم تشغيله على الجهاز الخاص بك، نظرا لاحتمال أختلاف أنواع ملفات تحليل الملفات استنادا إلى إصدار نظام التشغيل AsyncOS.

أنواع الملفات التي يمكن إرسالها لتحليل الملف:

- يمكن حاليا إرسال أنواع الملفات التالية للتحليل: (كافة الإصدارات التي تدعم تحليل الملفات) الملفات التنفيذية ل Windows، على سبيل المثال ملفات .exe و .dll و .sys و .scr.تنسيق Adobe Portable Document Format

Microsoft و (Microsoft Office 97-2004 (OLE و (Microsoft Office 2007+ (Open XML و (PDF
Windows / DOS Executable وغيرها من أنواع الملفات التي يحتمل أن تكون ضارة.أنواع الملفات التي قمت بتحديدها للتحميل على صفحة إعدادات Anti-Ware و Reputation (لأمان الويب) أو صفحة إعدادات File Reputation and Analysis (لأمان البريد الإلكتروني.) يتضمن الدعم المبدئي ملفات PDF و Microsoft Office.(بداية في AsyncOS 9.7.1 لأمان البريد الإلكتروني) إذا قمت بتحديد خيار أنواع الملفات الأخرى التي يحتمل أن تكون ضارة، فإن ملفات Microsoft Office بالملحقات التالية المحفوظة بتنسيق XML أو :MHTML
ADE، ADP، ADN، ACCDB، ACCDT، MDB، CDB، MDA، MDN، MDW، MDF، MDE، ACCDE،
dot، docx، dotx، dotm، DOCB، XL، XLT، MLXLX، xlsm، xltx، xltm، xlsb، xla، مستند، MAF، LDB
xlam، xll، xlw، ppt، port، pps، pptx، pptm، potx، potm، ppam، ppsx، ppsm، sldx، sldm، mhtm،
mhtml، و xml.

ملاحظة: إذا تجاوز الحمل الموجود على خدمة تحليل الملفات السعة، فقد لا يتم تحليل بعض الملفات حتى إذا تم تحديد نوع الملف للتحليل وكان الملف، لولا ذلك، مؤهلا للتحليل. سوف تتلقى تنبيها عندما تكون الخدمة غير قادرة مؤقتا على معالجة ملفات من نوع معين.

تمييز الملاحظات المهمة:

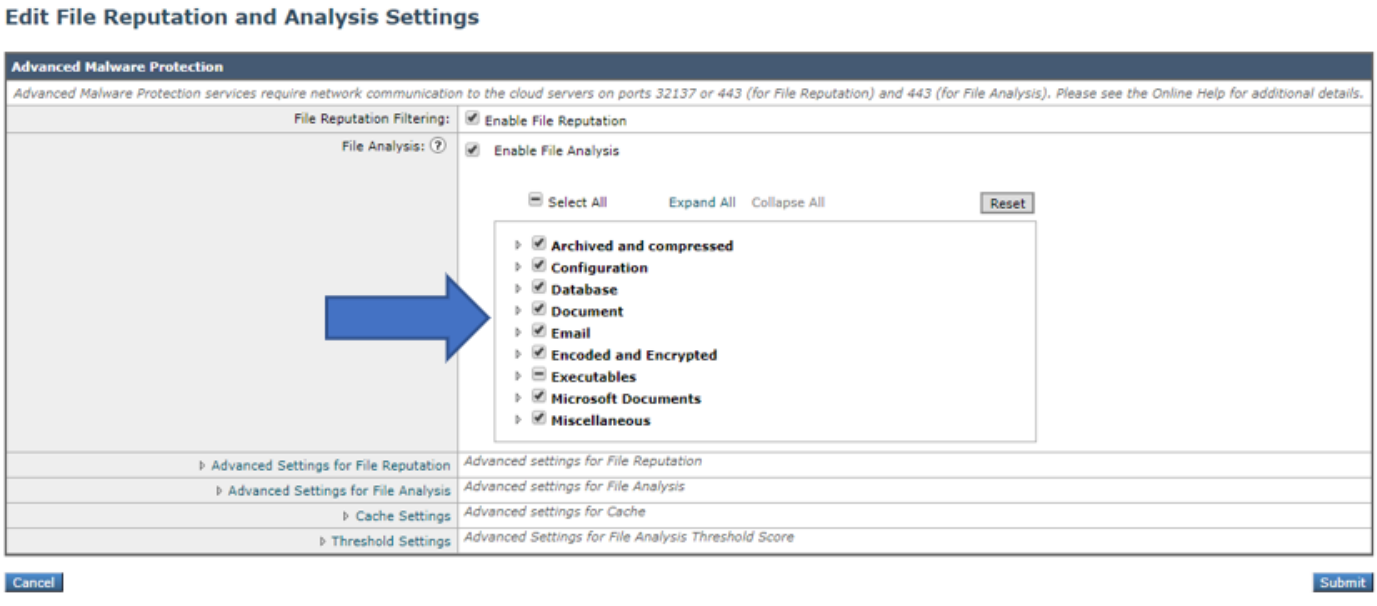
- إذا تم مؤخرا تحميل ملف من أي مصدر، فلن يتم تحميل الملف مرة أخرى. للحصول على نتائج تحليل الملف لهذا الملف، ابحث عن SHA-256 من صفحة تقارير تحليل الملفات.
- سيحاول الجهاز مرة واحدة تحميل الملف؛ إذا لم ينجح التحميل، على سبيل المثال بسبب مشاكل الاتصال، فقد لا يتم تحميل الملف. إذا كان الفشل بسبب تحميل خادم تحليل الملفات بشكل زائد، ستتم محاولة التحميل مرة أخرى.

تكوين AMP لتحليل الملف

بشكل افتراضي، عند تشغيل ESA لأول مرة ولم يقم بإنشاء اتصال بمحدث Cisco، يكون نوع ملف تحليل الملفات الوحيد المدرج هو ملفات "Microsoft Windows / DOS Executable". ستحتاج إلى السماح بإكمال تحديث الخدمة قبل السماح لك بتكوين أنواع ملفات إضافية. وسينعكس ذلك في ملف سجل updater_log، الذي يظهر على أنه "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
```

لتكوين تحليل الملفات عبر واجهة المستخدم الرسومية، انتقل إلى **خدمات الأمان > سمعة الملف وتحليله > تحرير الإعدادات العامة...**



دخلت in order to شكلت AMP ل مبرد تحليل عبر ال CLI، **ال ampconfig>setup** أمر وانتقلت من خلال الإستجابة معالج. يجب تحديد **Y** عند تقديم هذا السؤال: **هل تريد تعديل أنواع الملفات لتحليل الملفات؟**

```
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

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

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
ALL <[1,2,3,4,5]

(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
```

استنادا إلى هذا التكوين، تخضع أنواع الملفات التي تم تمكينها لتحليل الملفات، حسب الاقتضاء.

مراجعة سجلات AMP لتحليل الملفات

عندما يتم مسح المرفقات ضوئيا بواسطة File Reputation (سمعة الملف) أو تحليل الملف على ESA، فإنها تسجل في سجل AMP. لمراجعة هذا السجل لكل إجراءات AMP، قم بتشغيل **amp** من واجهة سطر الأوامر (CLI) الخاصة ب ESA أو قم بالتنقل خلال معالج الاستجابة سواء للأمر **tail** أو **grep**. يكون أمر **GREP** مفيدا إذا كنت تعرف الملف المحدد أو تفاصيل أخرى والتي تريد البحث عنها في سجل AMP.

فيما يلي مثال:

```
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
```

ملاحظة: تعرض الإصدارات الأقدم من AsyncOS" amp_watchdog.txt" في سجلات AMP. هذا ملف نظام تشغيل يتم عرضه كل عشر دقائق في السجلات. يعد هذا الملف جزءا من AMP الدائم وقد يتم تجاهله بأمان. هذا الملف مخفي بدءا من AsyncOS 10.0.1 والإصدارات الأحدث.

ملاحظة: ستسجل الإصدارات الأقدم من AsyncOS أن العلامة upload_action تحتوي على ثلاث قيم تم تعريفها لسلوك تحميل إلى تحليل الملف.

الاستجابات الثلاث لإجراء التحميل على AsyncOS الأقدم:

- "upload_action = 0": الملف معروف لخدمة Reputation؛ لا تقم بالإرسال للتحليل.
- upload_action = 1": send"
- "upload_action = 2": الملف معروف لخدمة Reputation؛ لا تقم بالإرسال للتحليل

استجابتان لإجراء التحميل على الإصدار x.12 من AsyncOS وما بعده:

- "upload_action = مستحسن إرسال الملف للتحليل"

• **سجلات التصحيح فقط:** "upload_action = مستحسن عدم إرسال الملف للتحليل"

تملي هذه الاستجابة ما إذا كان يتم إرسال ملف للتحليل أم لا. ومرة أخرى، يجب أن يستوفي معايير أنواع الملفات التي تم تكوينها حتى يتم إرساله بنجاح.

شرح علامات إجراء التحميل

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

بالنسبة إلى "0"، يعني ذلك أن الملف "غير ضروري للتحميل". أو، طريقة أفضل للنظر إليها هي، *يمكن* إرسال الملف للتحميل إلى تحليل الملف *إذا* لزم الأمر. ومع ذلك، إذا *لم* يكن الملف مطلوبا، فلن يتم إرسال الملف.

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

بالنسبة إلى "2"، هذا هو ملف "لا تقم بإرسال" ملف للتحميل بشكل صارم. هذا الإجراء نهائي وحاسم، ويتم معالجة تحليل الملفات.

أمثلة السيناريوهات

يصف هذا القسم السيناريوهات المحتملة التي يتم فيها تحميل الملفات للتحليل بشكل صحيح أو عدم تحميلها لسبب محدد.

تم تحميل الملف للتحليل

نظام التشغيل AsyncOS القديم:

يوضح هذا المثال ملف DOCX الذي يتوافق مع المعايير وتم وضع علامة عليه باستخدام **upload_action = 1**. في السطر التالي، يتم تسجيل **الملف الذي تم تحميله** للتحليل خوارزمية التجزئة الآمنة (SHA) في سجل AMP أيضا.

```
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 وما بعده:

يوضح هذا المثال ملف PPTX الذي يفي بالمعايير ويوضع عليه علامة باستخدام **upload_action = مستحسن إرسال الملف للتحليل**. في السطر التالي، يتم تسجيل **الملف الذي تم تحميله** للتحليل خوارزمية التجزئة الآمنة (SHA) في سجل AMP أيضا.

```
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
```

لم يتم تحميل الملف للتحليل لأن الملف معروف بالفعل

نظام التشغيل AsyncOS القديم:

يوضح هذا المثال ملف PDF تم مسحه ضوئيا بواسطة AMP مع **Upload_action = 2** ملحقة بسجل سمعة الملف. هذا الملف معروف مسبقا للسحابة ولا يلزم تحميله للتحليل، لذلك لا يتم تحميله مرة أخرى.

```
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 وما بعده:

يوضح هذا المثال ملف amp_watchdog.txt الذي يحتوي على سجلات AMP على مستوى تصحيح الأخطاء ويطابق **upload_action = مستحسن عدم إرسال الملف للتحليل** المضاف إلى سجل سمعة الملف. هذا الملف معروف مسبقا للسحابة ولا يلزم تحميله للتحليل، لذلك لا يتم تحميله مرة أخرى.

```
    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
```

تحميل تحليل ملف التسجيل عبر رؤوس البريد الإلكتروني

من واجهة سطر الأوامر (CLI)، مع الخيار باستخدام الأمر **logconfig**، يمكن تحديد الخيار الفرعي **loghaders** لسرد رؤوس رسائل البريد الإلكتروني التي تمت معالجتها عبر ESA وتسجيلها. باستخدام رأس "X-AMP-File-Upload"، في أي وقت يتم تحميل ملف أو عدم تحميله لتحليل الملف، سيتم تسجيله على سجلات بريد ESA.

عند النظر إلى سجلات البريد، نتائج الملفات التي تم تحميلها للتحليل:

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

عند النظر إلى سجلات البريد، نتائج الملفات التي لم يتم تحميلها للتحليل:

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

معلومات ذات صلة

- أدلة مستخدم AsyncOS
- معايير الملفات لخدمات الحماية المتقدمة من البرامج الضارة لمنتجات أمان المحتوى من Cisco
- إختبار ESA للحماية المتقدمة من البرامج الضارة (AMP)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).