Überprüfen von Dateianalyse-Uploads auf der ESA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie bestimmen können, ob Dateien, die über Advanced Malware Protection (AMP) auf der Cisco E-Mail Security Appliance (ESA) verarbeitet werden, zur Dateianalyse gesendet werden und welche Informationen die zugehörige AMP-Protokolldatei bietet.

Bestimmen, ob Anhänge zur Dateianalyse hochgeladen werden

Wenn die Dateianalyse aktiviert ist, können Anhänge, die mit Dateireputation gescannt werden, zur weiteren Analyse an die Dateianalyse gesendet werden. Dadurch wird ein Höchstmaß an Schutz vor Zero-Day- und gezielten Bedrohungen gewährleistet. Die Dateianalyse ist nur verfügbar, wenn die Dateireputationsfilterung aktiviert ist.

Verwenden Sie die Optionen Dateitypen, um die Dateitypen zu beschränken, die an die Cloud gesendet werden können. Die spezifischen Dateien, die gesendet werden, basieren immer auf Anforderungen aus der File Analysis Services Cloud, die auf die Dateien abzielt, für die zusätzliche Analysen erforderlich sind. Die Dateianalyse für bestimmte Dateitypen kann vorübergehend deaktiviert werden, wenn die Dateianalyse-Services-Cloud die Kapazität erreicht.

> **Hinweis**: Im Cisco Dokument File Criteria for Advanced Malware Protection Services for Cisco Content Security Products finden Sie aktuelle und zusätzliche Informationen.

> **Hinweis**: Bitte lesen Sie die Versionshinweise und das Benutzerhandbuch für die spezifische Version von AsyncOS, die auf Ihrer Appliance ausgeführt wird, da die Dateianalyse-Dateitypen je nach Version von AsyncOS variieren können.

Dateitypen, die zur Dateianalyse gesendet werden können:

- Die folgenden Dateitypen können derzeit zur Analyse gesendet werden: (Alle Releases, die Dateianalyse unterstützen) Ausführbare Windows-Dateien, z. B. .exe-, .dll-, .sys- und .scr-Dateien.Adobe Portable Document Format (PDF), Microsoft Office 2007+ (Open XML), Microsoft Office 97-2004 (OLE), Microsoft Windows/DOS Executable, andere potenziell schädliche Dateitypen.Dateitypen, die Sie für den Upload auf die Seite Anti-Malware- und Reputationseinstellungen (für Web Security) oder die Seite Dateireputation und Analyse (für E-Mail-Sicherheit) ausgewählt haben. Die erste Unterstützung umfasst PDF- und Microsoft Office-Dateien.(Beginnend in AsyncOS 9.7.1 for Email Security) Wenn Sie die Option Andere potenziell bösartige Dateitypen ausgewählt haben, werden Microsoft Office-Dateien mit den folgenden Erweiterungen im XML- oder MHTML-Format gespeichert: ade, adp, and, accdb, accdr, accdt, accda, mdb, cdb, mda, mdn, mdt, mdw, mdf, mde, accde, mam, maq, mar, mat, maf, ldb, laccdb, doc, dot, docx, docm, dotm, docb, xls, xlxls, xlxlx t, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, pot, pps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtml und xml.

  Hinweis: Wenn die Auslastung des Dateianalyseservice die Kapazität überschreitet, werden einige Dateien möglicherweise nicht analysiert, selbst wenn der Dateityp für die Analyse ausgewählt wurde und die Datei ansonsten für die Analyse geeignet wäre. Sie erhalten eine Warnung, wenn der Dienst vorübergehend nicht in der Lage ist, Dateien eines bestimmten Typs zu verarbeiten.

Wichtige Punkte:

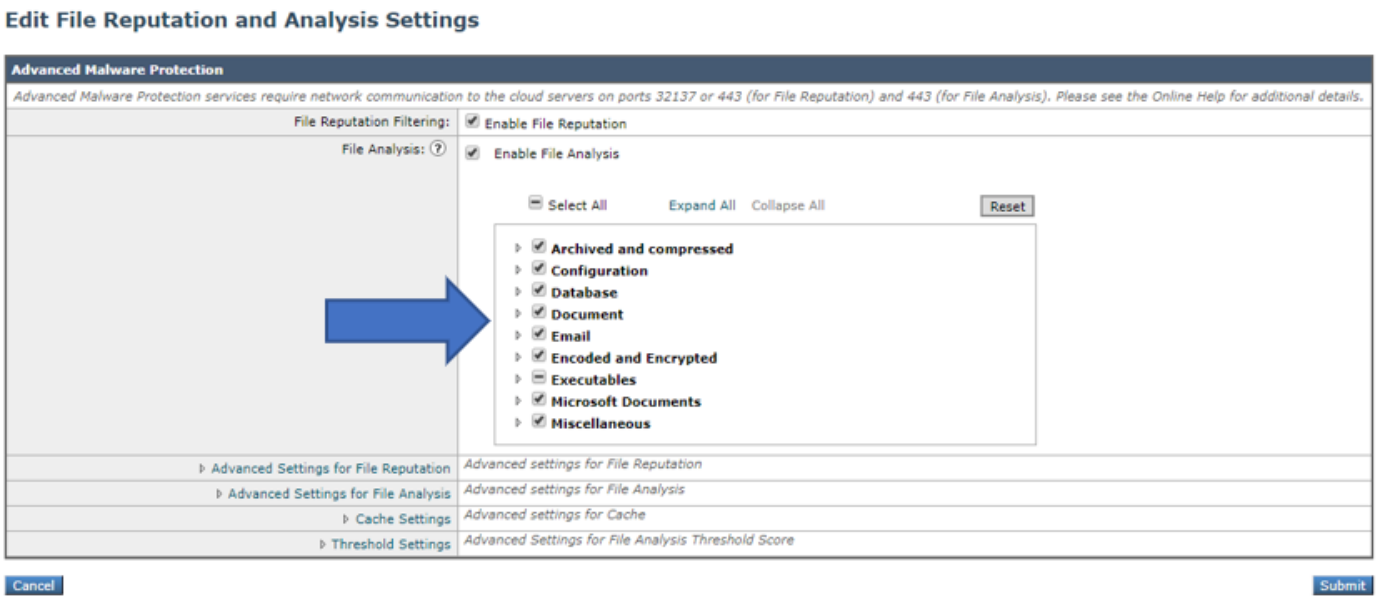
- Wenn vor kurzem eine Datei aus einer beliebigen Quelle hochgeladen wurde, wird die Datei nicht erneut hochgeladen. Suchen Sie auf der Reporting-Seite Dateianalyse nach den SHA-256-Ergebnissen für diese Datei.
- Die Appliance versucht einmal, die Datei hochzuladen. Wenn der Upload nicht erfolgreich ist, z. B. aufgrund von Verbindungsproblemen, wird die Datei möglicherweise nicht hochgeladen. Wenn der Fehler darin bestand, dass der Dateianalyseserver überlastet wurde, wird der Upload erneut versucht.

Konfigurieren von AMP für die Dateianalyse

Wenn eine ESA zum ersten Mal eingeschaltet wird und noch keine Verbindung zum Cisco Updater herstellen muss, werden standardmäßig als EINZIGE Dateianalyse-Dateityp "Microsoft Windows/DOS Executable" angegeben. Bevor Sie weitere Dateitypen konfigurieren können, müssen Sie ein Service-Update zulassen. Dies spiegelt sich in der Protokolldatei updater_logs wider, die als "fireamp.json" bezeichnet wird:

```
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"
```

Um die Dateianalyse über die Benutzeroberfläche zu konfigurieren, wählen Sie **Sicherheitsdienste > Dateireputation und Analyse > Globale Einstellungen bearbeiten..**



Um AMP für die Dateianalyse über die CLI zu konfigurieren, geben Sie den Befehl **ampconfig > setup** ein, und navigieren Sie durch den Antwortassistenten. Sie müssen **Y** auswählen, wenn Ihnen die folgende Frage angezeigt wird: **Möchten Sie die Dateitypen für die Dateianalyse ändern?**

```
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.
```

Basierend auf dieser Konfiguration unterliegen die aktivierten Dateitypen der Dateianalyse.

Überprüfen von AMP-Protokollen für die Dateianalyse

Wenn Anhänge auf der ESA nach Dateireputation oder Dateianalyse gescannt werden, werden sie im AMP-Protokoll erfasst. Um dieses Protokoll für alle AMP-Aktionen zu überprüfen, führen Sie die **Tail-AMP-Aktion** in der Kommandozeile der ESA aus, oder navigieren Sie durch den Antwortassistenten für den Befehl **tail** oder **grep**. Der **grep**-Befehl ist nützlich, wenn Sie die Datei oder andere Details kennen, für die Sie im AMP-Protokoll suchen möchten.

Hier ein Beispiel:

```
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
```

> **Hinweis**: Ältere Versionen von AsyncOS zeigen "amp_watchdog.txt" in den AMP-Protokollen an. Dies ist eine Betriebssystemdatei, die alle zehn Minuten in den Protokollen angezeigt wird. Diese Datei ist Teil der Keep-Alive für AMP und kann sicher ignoriert werden. Diese Datei ist ab AsyncOS 10.0.1 ausgeblendet.

> **Hinweis**: Ältere Versionen von AsyncOS protokollieren das upload_action-Tag mit drei Werten, die für das Upload in das Dateianalyseverhalten definiert sind.

Die drei Antworten für Upload-Aktionen auf älteren AsyncOS-Betriebssystemen:

- "upload_action = 0": Die Datei ist dem Reputationsdienst bekannt. senden Sie nicht zur Analyse.

- "upload_action = 1": Senden
- "upload_action = 2": Die Datei ist dem Reputationsdienst bekannt. Senden Sie keine Analyse.

Die beiden Antworten für Upload-Aktionen auf AsyncOS Version 12.x und höher:

- "upload_action = Empfohlen, die Datei zur Analyse zu senden"
- **Nur Debug-Protokolle:** "upload_action = Empfohlen, die Datei nicht zur Analyse zu senden"

Diese Antwort gibt an, ob eine Datei zur Analyse gesendet wird. Auch hier muss er die Kriterien der konfigurierten Dateitypen erfüllen, damit er erfolgreich übermittelt werden kann.

Erklärung zum Hochladen von Action-Tags

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`
Für "0" bedeutet dies, dass die Datei "nicht zum Upload gesendet werden muss". Alternativ dazu *kann* die Datei *bei* Bedarf zur Dateianalyse hochgeladen werden. Wenn die Datei jedoch *nicht* erforderlich ist, wird sie nicht gesendet.

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`
Für "2" ist dies eine strikte "nicht senden" die Datei zum Hochladen. Diese Aktion ist endgültig und entscheidend, und die Dateianalyse wird verarbeitet.

Beispielszenarien

In diesem Abschnitt werden mögliche Szenarien beschrieben, in denen Dateien entweder ordnungsgemäß zur Analyse hochgeladen werden oder aus einem bestimmten Grund nicht hochgeladen werden.

Datei zur Analyse hochgeladen

Älteres AsyncOS:

Dieses Beispiel zeigt eine DOCX-Datei, die die Kriterien erfüllt und mit dem **upload_action = 1** gekennzeichnet ist. In der nächsten Zeile wird die **Datei**, **die zur Analyse** von Secure Hash Algorithm (SHA) hochgeladen wurde, ebenfalls in das AMP-Protokoll aufgenommen.

```
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 und höher:

Dieses Beispiel zeigt eine PPTX-Datei, die die Kriterien erfüllt und mit dem **upload_action = Empfohlen** gekennzeichnet ist**, um die Datei zur Analyse zu senden**. In der nächsten Zeile wird die **Datei**, **die zur Analyse** von Secure Hash Algorithm (SHA) hochgeladen wurde, ebenfalls in das AMP-Protokoll aufgenommen.

```
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
```

Datei wurde nicht zur Analyse hochgeladen, da die Datei bereits bekannt ist

Älteres AsyncOS:

Dieses Beispiel zeigt eine PDF-Datei, die von AMP gescannt wird, wobei **upload_action = 2** an das Dateireputationsprotokoll angehängt wird. Diese Datei ist bereits der Cloud bekannt und muss nicht zur Analyse hochgeladen werden. Daher wird sie nicht erneut hochgeladen.

```
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 und höher:

Dieses Beispiel zeigt die Datei amp_watchdog.txt mit AMP-Protokollen auf Debugebene, die der **Datei upload_action = Empfohlen ist, die Datei nicht zur Analyse** an das Dateireputationsprotokoll angehängt **zu senden**. Diese Datei ist bereits der Cloud bekannt und muss nicht zur Analyse hochgeladen werden. Daher wird sie nicht erneut hochgeladen.

```
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
```

Hochladen der Dateianalyse über E-Mail-Header

In der CLI kann mit der Option **logconfig** die Unteroption **Logheaders** ausgewählt werden, um die Header von E-Mails aufzulisten und zu protokollieren, die über die ESA verarbeitet werden. Mit dem Header "X-Amp-File-Uploaded" wird jedes Mal, wenn eine Datei hochgeladen oder nicht zur Dateianalyse hochgeladen wird, in die E-Mail-Protokolle der ESA aufgenommen.

Überprüfen Sie die E-Mail-Protokolle, die Ergebnisse für zur Analyse hochgeladene Dateien:

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

Überprüfen Sie die E-Mail-Protokolle, die Ergebnisse für Dateien, die nicht zur Analyse hochgeladen wurden:

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

Zugehörige Informationen

- AsyncOS-Benutzerhandbücher
- Dateikriterien für Advanced Malware Protection Services für Cisco Content Security-Produkte
- ESA Advanced Malware Protection (AMP)-Test
- Technischer Support und Dokumentation - Cisco Systems