Verifica del caricamento dell'analisi dei file su ESA

Sommario

Introduzione

In questo documento viene descritto come determinare se i file elaborati tramite Advanced Malware Protection (AMP) su Cisco Email Security Appliance (ESA) vengono inviati per l'analisi dei file e cosa fornisce il file di registro AMP associato.

Verifica del caricamento degli allegati per l'analisi dei file

Se l'analisi dei file è attivata, gli allegati analizzati da File Reputation possono essere inviati all'analisi dei file per ulteriori analisi. In questo modo è possibile ottenere il massimo livello di protezione contro le minacce a giornata zero e mirate. L'analisi dei file è disponibile solo quando il filtro reputazione file è abilitato.

Utilizzare le opzioni Tipi di file per limitare i tipi di file che possono essere inviati al cloud. I file specifici inviati sono sempre basati sulle richieste provenienti dal cloud di File Analysis Services, che ha come destinazione i file per i quali è necessaria un'analisi aggiuntiva. L'analisi dei file per determinati tipi di file potrebbe essere disabilitata temporaneamente quando il cloud di Servizi di analisi file raggiunge la capacità.

> **Nota:** Per ulteriori informazioni, consultare il documento Criteri file per i servizi avanzati di protezione dal malware per i prodotti Cisco Content Security.

> **Nota:** Consultare le note sulla versione e la guida per l'utente per la revisione specifica di AsyncOS in esecuzione sull'accessorio, in quanto i tipi di file per l'analisi dei file possono variare a seconda della versione di AsyncOS.

Tipi di file che è possibile inviare per l'analisi dei file:

- I seguenti tipi di file possono essere attualmente inviati per l'analisi: (Tutte le versioni che

supportano l'analisi dei file) File eseguibili di Windows, ad esempio file con estensione exe, dll, sys e scr.Adobe Portable Document Format (PDF), Microsoft Office 2007+ (Open XML), Microsoft Office 97-2004 (OLE), Eseguibile Microsoft Windows / DOS, Altri tipi di file potenzialmente dannosi.Tipi di file selezionati per il caricamento nella pagina Impostazioni antimalware e reputazione (per Web Security) o nella pagina Impostazioni reputazione e analisi file (per Email Security). Il supporto iniziale include file PDF e Microsoft Office.(A partire da AsyncOS 9.7.1 for Email Security) Se è stata selezionata l'opzione Altri tipi di file potenzialmente dannosi, i file di Microsoft Office con le seguenti estensioni vengono salvati in formato XML o MHTML: ade, adp, and, accdb, accdr, accdt, accda, mdb, cdb, mda, mdn, mdt, mdf, mde, accde, mam, maq, mar, mat, maf, ldb, laccdb, doc, dot, docx, docm, dotx, dotm, docb, xls, xlt, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlpw, ppt, ps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtm, mhtml e xml.

Nota: Se il carico sul servizio Analisi file supera la capacità, alcuni file potrebbero non essere analizzati anche se il tipo di file è selezionato per l'analisi e il file sarebbe altrimenti idoneo per l'analisi. Quando il servizio non è temporaneamente in grado di elaborare file di un determinato tipo, viene visualizzato un avviso.

Evidenziare le note importanti:

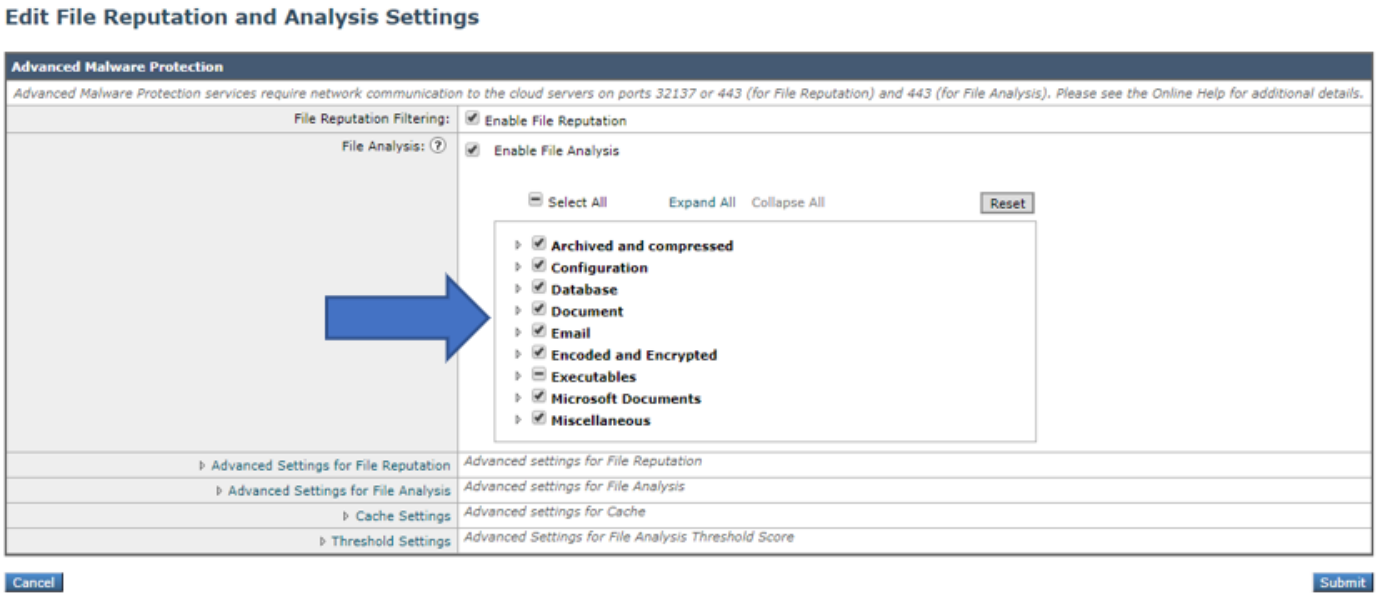
- Se un file è stato caricato di recente da qualsiasi origine, non verrà caricato di nuovo. Per i risultati dell'analisi del file, cercare SHA-256 dalla pagina Report analisi file.
- L'accessorio tenterà una volta di caricare il file; se il caricamento non riesce, ad esempio a causa di problemi di connettività, il file potrebbe non essere caricato. Se l'errore è dovuto al sovraccarico del file analysis server, verrà eseguito un nuovo tentativo di caricamento.

Configurazione di AMP per l'analisi dei file

Per impostazione predefinita, quando un'ESA è accesa per la prima volta e non è ancora stata stabilita una connessione al programma di aggiornamento Cisco, il tipo di file dell'analisi dei file ONLY elencato è "Microsoft Windows / DOS Executable". È necessario consentire il completamento di un aggiornamento del servizio prima di poter configurare altri tipi di file. Ciò si rifletterà nel file di log updater_logs, visualizzato come "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"
```

Per configurare l'analisi dei file dalla GUI, selezionare **Security Services > File Reputation and Analysis > Edit Global Settings...**



Per configurare AMP for File Analysis dalla CLI, immettere il comando **ampconfig > setup** e passare alla procedura guidata di risposta. È necessario selezionare **Y** quando viene visualizzata la seguente domanda: **Modificare i tipi di file per l'analisi dei file?**

```
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.
```

In base a questa configurazione, i tipi di file abilitati sono soggetti all'analisi dei file, se applicabile.

Esamina log AMP per analisi file

Gli allegati scansionati mediante Reputazione file o Analisi file sull'ESA vengono registrati nel registro AMP. Per esaminare questo log per tutte le azioni AMP, eseguire **tail amp** dalla CLI dell'ESA o spostarsi nella procedura guidata di risposta per il comando **tail** o **grep**. Il comando **grep** è utile se si conosce il file specifico o altri dettagli da cercare nel log AMP.

Di seguito è riportato un esempio:

```
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
```

> **Nota:** Le versioni precedenti di AsyncOS visualizzano "amp_watchdog.txt" nei registri AMP. Si tratta di un file del sistema operativo che viene visualizzato ogni dieci minuti nei log. Questo file fa parte del keep-alive per AMP e può essere ignorato. Questo file è nascosto a partire da AsyncOS 10.0.1 e versioni successive.

> **Nota:** Nelle versioni precedenti di AsyncOS, il tag upload_action viene registrato con tre valori definiti per il comportamento dell'analisi di caricamento su file.

Le tre risposte per l'azione di caricamento su AsyncOS meno recenti:

- "upload_action = 0": Il file è noto al servizio di reputazione; non inviare per l'analisi.
- "upload_action = 1": Invio
- "upload_action = 2": Il file è noto al servizio di reputazione; non inviare per l'analisi

Le due risposte per l'azione di caricamento su AsyncOS versione 12.x e successive:

- "upload_action = Consigliato per inviare il file per l'analisi"
- **Solo log di debug:** "upload_action = Consigliato di non inviare il file per l'analisi"

Questa risposta determina se un file viene inviato per l'analisi. Anche in questo caso, per essere inviato correttamente, deve soddisfare i criteri dei tipi di file configurati.

Spiegazione dei tag di azione caricamento

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`
Per "0," significa che il file "non deve essere inviato per il caricamento". In alternativa, un modo migliore per esaminarlo è che il file *può* essere inviato per il caricamento nell'analisi dei file *se* necessario. Tuttavia, se il file *non* è necessario, il file non viene inviato.

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`
Per "2", si tratta di una stringa "non inviare" il file per il caricamento. Questa azione è definitiva e decisiva e l'elaborazione dell'analisi dei file viene eseguita.

Scenari di esempio

In questa sezione vengono descritti i possibili scenari in cui i file vengono caricati per l'analisi correttamente o non vengono caricati per un motivo specifico.

File caricato per l'analisi

AsyncOS precedente:

Nell'esempio viene mostrato un file DOCX che soddisfa i criteri ed è contrassegnato con **upload_action = 1**. Nella riga successiva, il **file caricato per l'analisi** con SHA (Secure Hash Algorithm) viene registrato anche nel log AMP.

```
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 e versioni successive:

Nell'esempio viene mostrato un file PPTX che soddisfa i criteri e a cui viene assegnato il tag **upload_action = Recommended per inviare il file per l'analisi**. Nella riga successiva, il **file caricato per l'analisi** SHA (Secure Hash Algorithm) viene registrato anche nel log AMP.

```
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
```

File non caricato per l'analisi perché è già noto

AsyncOS precedente:

Nell'esempio viene mostrato un file PDF analizzato da AMP con **upload_action = 2** aggiunto al log della reputazione del file. Questo file è già noto al cloud e non deve essere caricato per l'analisi, quindi non viene caricato di nuovo.

```
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 e versioni successive:

In questo esempio viene mostrato il file amp_watchdog.txt con i log amp a livello di debug corrispondenti a **upload_action = Consigliato di non inviare il file per l'analisi** aggiunto al log della reputazione del file. Questo file è già noto al cloud e non deve essere caricato per l'analisi, quindi non viene caricato di nuovo.

```
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
```

Registrazione dell'analisi dei file tramite le intestazioni e-mail

Dalla CLI, con l'opzione che usa il comando **logconfig**, è possibile selezionare l'opzione secondaria **logheaders** per elencare e registrare le intestazioni dei messaggi di posta elettronica elaborati tramite l'ESA. Usando l'intestazione "X-Amp-File-Uploaded", ogni volta che un file viene caricato o non caricato per l'analisi del file verrà registrato nei log di posta dell'ESA.

Esaminando i log di posta, i risultati per i file caricati per l'analisi:

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

Esaminando i log di posta, i risultati per i file non caricati per l'analisi:

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

Informazioni correlate

- Guide per l'utente AsyncOS
- Criteri file per i servizi avanzati di protezione malware per i prodotti Cisco Content Security
- Test ESA Advanced Malware Protection
- Documentazione e supporto tecnico – Cisco Systems