ESA에서 파일 분석 업로드 확인

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 AMP(Advanced Malware Protection)를 통해 처리되는 파일이 파일 분석을 위해 전송되는지 여부와 관련 AMP 로그 파일에서 제공하는 기능을 확인하는 방법에 대해 설명합니다.

첨부 파일이 파일 분석을 위해 업로드되었는지 확인

File Analysis(파일 분석)가 활성화되면 파일 평판으로 스캔되는 첨부 파일을 추가 분석을 위해 File Analysis(파일 분석)로 전송할 수 있습니다.이는 제로데이 및 표적 위협에 대한 최고 수준의 보호를 제공합니다.파일 분석은 파일 평판 필터링이 활성화된 경우에만 사용할 수 있습니다.

클라우드로 전송할 수 있는 파일 유형을 제한하려면 File Types 옵션을 사용합니다.전송되는 특정 파일은 항상 File Analysis services Cloud의 요청을 기반으로 하며, 추가 분석이 필요한 파일을 대상으로 합니다.File Analysis services Cloud가 용량에 도달하면 특정 파일 유형에 대한 파일 분석이 일시적으로 비활성화될 수 있습니다.

> **참고:**최신 정보와 추가 정보는 Cisco Content Security 제품에 대한 Advanced Malware Protection Services의 파일 기준 Cisco 문서를 참조하십시오.

> **참고:** AsyncOS 버전에 따라 파일 분석 파일 유형이 달라질 수 있으므로 어플라이언스에서 실행되는 AsyncOS의 특정 버전에 대해서는 릴리스 정보 및 사용 설명서를 검토하십시오.

파일 분석을 위해 보낼 수 있는 파일 유형:

- 분석을 위해 현재 다음 파일 유형을 보낼 수 있습니다. (파일 분석을 지원하는 모든 릴리스) Windows 실행 파일(예: .exe, .dll, .sys 및 .scr 파일)Adobe PDF(Portable Document Format), Microsoft Office 2007+(Open XML), Microsoft Office 97-2004(OLE), Microsoft Windows/DOS 실행 파일, 기타 악성 파일 형식Anti-Malware and Reputation 설정 페이지(Web Security용) 또는 File Reputation and Analysis 설정 페이지(Email Security용)에서 업로드하도록 선택한 파일

유형 초기 지원에는 PDF 및 Microsoft Office 파일이 포함됩니다.(AsyncOS 9.7.1 for Email Security에서 시작) [기타 잠재적으로 악의적인 파일 형식] 옵션을 선택한 경우 XML 또는 MHTML 형식으로 저장된 다음 확장명을 가진 Microsoft Office 파일입니다.ade, adp, accdb, accdr, accdt, accda, mdb, cdb, mda, mdn, mdw, mdw, mde, mde, mde, mad, mq, mad, mq, mat, ldb, lacdb, dot, dox, dotx, dotm, dotx, dotx, dotm, dotm, xlt, xlt, xlsd, xlsm, xlsx, xltm, xlsb, xlxlxltm, xlsb, xlxla, xlxllam, xlxllam, xllam, xlxlxllam, xllam, xlxlxlxllaw, xllam, xllaw, xllaw, xllaw, xllaw, xllaw, xllam, xl, xl, xllaw, xllaw, xllaw, xllaw, x포트, pps, pptx, pptm, potm, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtm, mhtml, xml,

참고:파일 분석 서비스의 로드가 용량을 초과할 경우 분석을 위해 파일 유형을 선택해도 일부 파일이 분석되지 않을 수 있으며, 그렇지 않을 경우 파일이 분석될 수 있습니다.서비스가 일시적으로 특정 유형의 파일을 처리할 수 없을 때 알림을 받게 됩니다.

중요 메모 강조 표시:

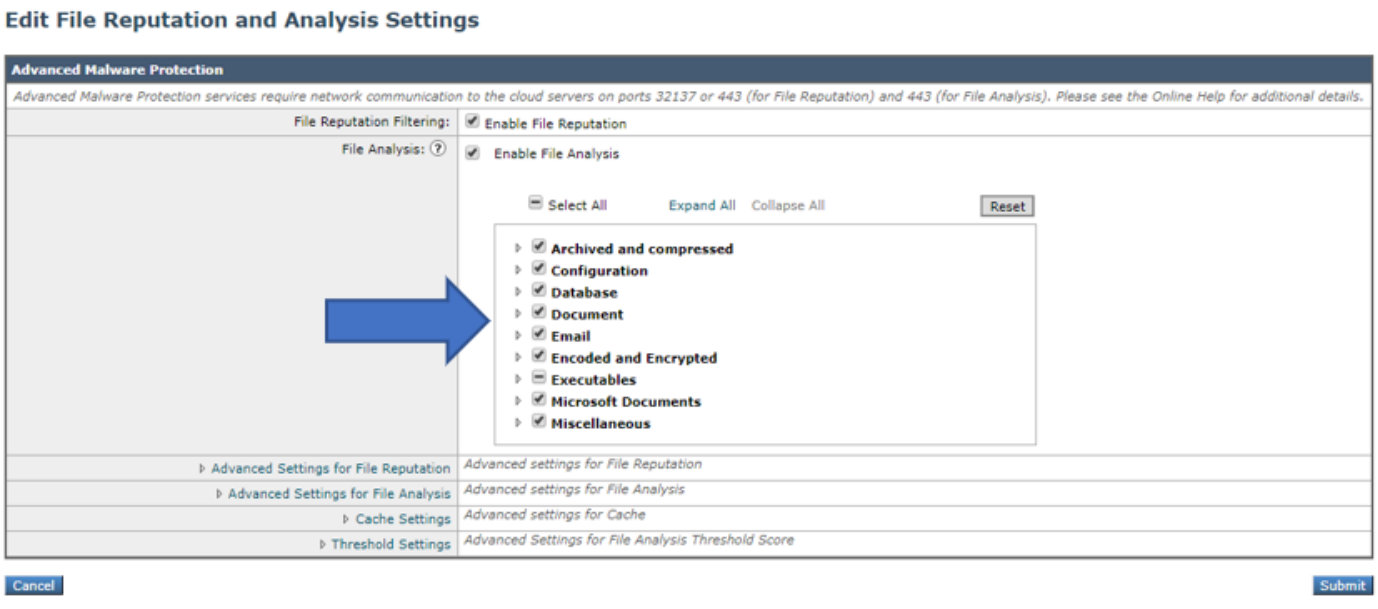
- 최근에 소스에서 파일을 업로드한 경우 파일이 다시 업로드되지 않습니다.이 파일에 대한 파일 분석 결과를 보려면 File Analysis(파일 분석) 보고 페이지에서 SHA-256을 검색합니다.
- 어플라이언스는 파일을 업로드하려고 한 번 시도합니다.업로드에 성공하지 못할 경우(예: 연결 문제로 인해) 파일이 업로드되지 않을 수 있습니다.파일 분석 서버가 오버로드되었기 때문에 오류가 발생한 경우 업로드를 다시 시도합니다.

파일 분석용 AMP 구성

기본적으로 ESA가 처음 켜져 있고 Cisco 업데이터와의 연결을 아직 설정하지 않은 경우 나열된 유일한 파일 분석 파일 유형은 "Microsoft Windows/DOS 실행 파일" 파일입니다. 추가 파일 유형을 구성하기 전에 서비스 업데이트가 완료되도록 허용해야 합니다. 이는 "fireamp.json"으로 표시되는 updater_logs 로그 파일에 반영됩니다.

```
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"
```

GUI를 통해 파일 분석을 구성하려면 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석) > Edit Global Settings(전역 설정 편집)로 이동합니다.**



CLI를 통해 AMP for File Analysis를 구성하려면 ampconfig **> setup** 명령을 입력하고 응답 마법사를 진행합니다.다음 질문이 표시되면 **Y**를 선택해야 합니다. **파일 분석을 위한 파일 유형을 수정하시겠습니까?**

```
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.
```

이 컨피그레이션에 따라 활성화되는 파일 유형은 File Analysis(파일 분석)의 적용을 받습니다.

파일 분석을 위한 AMP 로그 검토

ESA의 File Reputation(파일 평판) 또는 File Analysis(파일 분석)에서 첨부 파일을 스캔하면 AMP 로그에 기록됩니다.모든 AMP 작업에 대해 이 로그를 검토하려면 ESA CLI에서 **tail amp**를 실행하거나 **tail** 또는 grep 명령에 대한 응답 마법사를 거칩니다. **grep** 명령은 AMP 로그에서 검색하려는 특정 파일 또는 기타 세부사항을 알고 있는 경우 유용합니다.

예를 들면 다음과 같습니다.

```
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
```

> **참고:**이전 버전의 AsyncOS는 AMP 로그에 "amp_watchdog.txt"를 표시합니다. 로그에 10분마다 표시되는 OS 파일입니다.이 파일은 AMP용 Keep-Alive의 일부이며 무시해도 안전합니다. 이 파일은 AsyncOS 10.0.1 이상부터 숨겨집니다.

> **참고:**이전 버전의 AsyncOS는 upload_action 태그에 파일 분석 동작에 대한 업로드에 대해 정의된 세 가지 값이 있습니다.

이전 AsyncOS의 업로드 작업에 대한 3가지 응답:

- "upload_action = 0":파일이 평판 서비스에 알려져 있습니다.분석을 위해 보내지 마십시오.
- "upload_action = 1":보내기
- "upload_action = 2":파일이 평판 서비스에 알려져 있습니다.분석을 위해 보내지 않음

AsyncOS 버전 12.x 이상에서 업로드 작업에 대한 두 가지 응답:

- "upload_action = 분석을 위해 파일을 전송하는 것이 좋습니다."
- **디버그 로그만**: "upload_action = 분석을 위해 파일을 보내지 않는 것이 좋습니다."

이 응답은 분석을 위해 파일을 전송할지 여부를 결정합니다.다시 한 번, 성공적으로 제출하려면 구성된 파일 유형의 기준을 충족해야 합니다.

업로드 작업 태그 설명

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

"0"의 경우 "파일을 업로드하기 위해 전송할 필요가 없음"을 의미합니다. 또는 더 잘 볼 수 있는 방법은 필요한 *경우* 파일 분석으로 업로드하기 위해 파일을 보낼 수 있다는 것입니다. 그러나 파일이 *필요하지* 않으면 파일이 전송되지 않습니다.

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

"2"의 경우 이 파일은 업로드할 때 엄격한 "보내지 않음"입니다. 이 작업은 최종 결정이며 파일 분석 처리가 완료되었습니다.

예제 시나리오

이 섹션에서는 분석을 위해 파일이 제대로 업로드되거나 특정 이유로 업로드되지 않는 경우에 대해 설명합니다.

분석을 위해 업로드된 파일

이전 AsyncOS:

이 예에서는 기준을 충족하고 upload_**action = 1**으로 태그가 지정된 DOCX 파일을 보여 줍니다. 다음 행에서 **분석을 위해 업로드된 SHA**(Secure Hash Algorithm)가 AMP 로그에도 기록됩니다.

```
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 이상:

이 예에서는 기준을 충족하고 **분석을 위해 파일**을 **전송하기 위해 upload_action = Recommended**로 태그가 지정된 PPTX 파일을 보여 줍니다.다음 행에서 **분석** SHA(Secure Hash Algorithm)**를 위해 업로드된** 파일이 AMP 로그에도 기록됩니다.

```
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
```

파일이 이미 알려져 있으므로 분석을 위해 업로드되지 않음

이전 AsyncOS:

이 예에서는 AMP에서 스캔한 PDF 파일**과 upload_action = 2**가 파일 평판 로그에 추가된 것을 보여줍니다.이 파일은 이미 클라우드에 알려져 있으며 분석을 위해 업로드할 필요가 없으므로 다시 업로드되지 않습니다.

```
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 이상:

이 예에서는 **upload_action = Recommended not send the file for analysis** append to append log(**파일 평판** 로그에 추가된 **분석을 위해 파일을 보내지 않는 것이 좋습니다**. 디버그 레벨의 amp 로그가 포함된 amp_watchdog.txt 파일을 보여줍니다.이 파일은 이미 클라우드에 알려져 있으며 분석을 위해 업로드할 필요가 없으므로 다시 업로드되지 않습니다.

```
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
```

이메일 헤더를 통한 로깅 파일 분석 업로드

CLI에서 logconfig 명령을 사용하는 옵션과 함께 logheaders의 하위 옵션을 선택하여 ESA를 통해 처리된 이메일 헤더를 나열하고 기록할 수 있습니다. "X-Amp-File-Uploaded" 헤더를 사용하면 언제든지 파일이 업로드되거나 파일 분석을 위해 업로드되지 않을 때 ESA의 메일 로그에 기록됩니다.

메일 로그를 보면 분석을 위해 업로드된 파일에 대한 결과가 표시됩니다.

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

메일 로그를 보면 분석을 위해 업로드되지 않은 파일에 대한 결과가 표시됩니다.

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

관련 정보

- AsyncOS 사용자 가이드
- Cisco Content Security 제품에 대한 Advanced Malware Protection 서비스의 파일 기준
- ESA AMP(Advanced Malware Protection) 테스트
- 기술 지원 및 문서 – Cisco Systems