Verificando transferências de arquivo pela rede da análise do arquivo no ESA

Índice

[Introdução](#)
[Determine se os acessórios são transferidos arquivos pela rede para a análise do arquivo](#)
[Configurar o AMP para a análise do arquivo](#)
[Reveja logs AMP para a análise do arquivo](#)
[Explicação de etiquetas da ação da transferência de arquivo pela rede](#)
[Cenários de exemplo](#)
[Arquivo transferido arquivos pela rede para a análise](#)
[Arquivo não transferido arquivos pela rede para a análise porque o arquivo é sabido já](#)
[Transferência de arquivo pela rede da análise do arquivo de registro através dos encabeçamentos do email](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como determinar se os arquivos que são processados com a proteção avançada do malware (AMP) na ferramenta de segurança do email de Cisco (ESA) estão enviados para a análise do arquivo, e também o que o arquivo de registro associado AMP fornece.

Determine se os acessórios são transferidos arquivos pela rede para a análise do arquivo

Com arquivo a análise é permitida, os acessórios que são feitos a varredura pela reputação do arquivo podem ser enviados para arquivar a análise para a análise mais aprofundada. Isto fornece o mais de nível elevado da proteção contra o zero-dia e ameaças visadas. A análise do arquivo está somente disponível quando a filtração da reputação do arquivo é permitida.

Use as opções dos tipos de arquivo a fim limitar os tipos de arquivos que puderam ser enviados à nuvem. Os arquivos do específico que são enviados são baseados sempre em pedidos da nuvem dos serviços da análise do arquivo, que visa aqueles arquivos para que a análise adicional é precisada. A análise do arquivo para tipos de arquivo particulares pôde ser desabilitada temporariamente em que a análise do arquivo presta serviços de manutenção à capacidade dos alcances da nuvem.

> Nota: Refira os critérios do arquivo para serviços de proteção avançados do malware para o documento Cisco dos produtos de segurança do índice de Cisco para o mais atualizado e informação adicional.

> Nota: Reveja por favor os Release Note e o Guia do Usuário para a revisão específica de AsyncOS que é executado em seu dispositivo, porque os tipos de arquivo da análise do

arquivo podem variar baseado na versão de AsyncOS.

Tipos de arquivo que podem ser enviados para a análise do arquivo:

- Os seguintes tipos de arquivo podem atualmente ser enviados para a análise: (Todas as liberações que apoiam a análise do arquivo) Windows executáveis, arquivos por exemplo do .exe, do .dll, .sys, e .scr.Formato de documento portátil de Adobe (PDF), microsoft office 2007+ (XML aberto), microsoft office 97-2004 (OLE), Microsoft Windows/DOS executável, outros tipos de arquivo potencialmente maliciosos.Tipos de arquivo que você selecionou para a transferência de arquivo pela rede página nos ajustes do Anti-malware e da reputação (para a Segurança da Web) ou página dos ajustes da reputação e da análise do arquivo (para a Segurança do email.) O suporte inicial inclui o PDF e os arquivos do microsoft office.(Começo em AsyncOS 9.7.1 para a Segurança do email) se você selecionou a outra opção potencialmente maliciosa dos tipos de arquivo, o microsoft office arquiva com os seguintes Ramais salvar no formato XML ou MHTML: ade, adp, ADN, accdb, accdr, accdt, accda, mdb, cdb, mda, mdn, mdt, mdw, mdf, mde, accde, mam, maq, março, esteira, maf, ldb, laccdb, doc, ponto, docx, docm, dotx, dotm, docb, xls, xlt, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, potenciômetro, pps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtm, mhtml, e xml.

  Nota: Se a carga no serviço da análise do arquivo excede a capacidade, alguns arquivos não podem ser analisados mesmo se o tipo de arquivo é selecionado para a análise e o arquivo seria de outra maneira elegível para a análise. Você receberá um alerta quando o serviço é temporariamente incapaz de processar arquivos de um tipo particular.

Destacando observações importantes:

- Se um arquivo tem sido transferido arquivos pela rede recentemente de qualquer fonte, o arquivo não estará transferido arquivos pela rede outra vez. Para resultados da análise do arquivo para este arquivo, busca para o SHA-256 da página do relatório da análise do arquivo.
- O dispositivo tentará uma vez transferir arquivos pela rede o arquivo; se a transferência de arquivo pela rede não é bem sucedida, por exemplo devido aos problemas de conectividade, o arquivo não pode ser transferido arquivos pela rede. Se a falha era porque o server da análise do arquivo foi sobrecarregado, a transferência de arquivo pela rede será tentada uma vez mais.

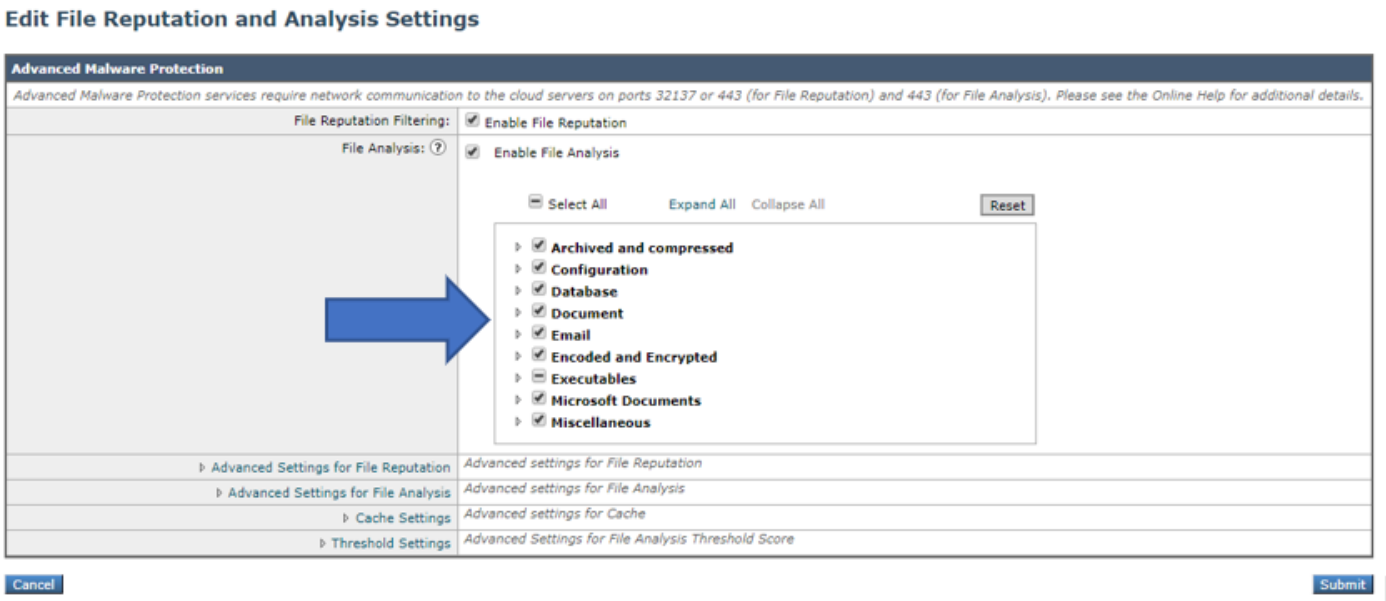
Configurar o AMP para a análise do arquivo

Àrevelia, quando um ESA é girado primeiramente sobre e tem para estabelecer ainda uma conexão ao updater de Cisco, o ÚNICO tipo de arquivo da análise do arquivo alistado será de “arquivos executáveis Microsoft Windows/DOS”. Você precisará de permitir que uma atualização do serviço termine antes de ser reservada configurar tipos de arquivo adicionais. Isto será refletido no arquivo de registro dos updater_logs, visto como “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"
```

Para configurar a análise do arquivo através do GUI, navegue aos **Serviços de segurança > à reputação do arquivo e a análise > edita configurações globais…**



A fim configurar o AMP para a análise do arquivo através do CLI, incorpore o **ampconfig > o comando setup** e o movimento através do assistente da resposta. Você deve selecionar **Y** quando você é presentado com esta pergunta: **Você quer alterar os tipos de arquivo para a análise do arquivo?**

```
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.
```

Baseado nesta configuração, os tipos de arquivo que são permitidos são sujeitos arquivar a análise, como aplicável.

Logs da revisão AMP para a análise do arquivo

Quando os acessórios são feitos a varredura pela reputação do arquivo ou arquivam a análise no ESA, estão gravados no log AMP. A fim rever este log para todas as ações AMP, execute a **cauda ampère do** CLI do ESA, ou mova-se através do assistente da resposta para a **cauda** ou o **comando grep**. **O comando grep** é útil se você conhece o arquivo específico ou outros detalhes por que você deseja procurar no log AMP.

Aqui está um exemplo:

```
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: Umas versões mais velhas de AsyncOS indicariam “amp_watchdog.txt” nos logs AMP. Este é um arquivo do OS que seja indicado cada dez minutos nos logs. Este arquivo é parte da manutenção de atividade para o AMP e pode com segurança ser ignorado. Este arquivo está começando hidden em AsyncOS 10.0.1 e mais novo.

> Nota: Umas versões mais velhas de AsyncOS registrarão a etiqueta do upload_action têm três valores que é definida para que a transferência de arquivo pela rede arquive o

comportamento da análise.

As três respostas para a ação da transferência de arquivo pela rede em AsyncOS mais velho:

- “upload_action = 0": O arquivo é sabido ao serviço da reputação; não envie para a análise.
- “upload_action = 1": Envie
- “upload_action = 2": O arquivo é sabido ao serviço da reputação; não envie para a análise

As duas respostas para a ação da transferência de arquivo pela rede na versão 12.x de AsyncOS e avante:

- o “upload_action = recomendou enviar o arquivo para a análise”
- **Debugar logs somente:** o “upload_action = recomendou não enviar o arquivo para a análise”

Esta resposta dita se um arquivo está enviado para a análise. Além disso, deve encontrar os critérios dos tipos de arquivo configurados a fim ser submetido com sucesso.

Explicação de etiquetas da ação da transferência de arquivo pela rede

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`
Para "0," isto significa que o arquivo “não está precisado de ser enviado para a transferência de arquivo pela rede”. Ou, uma maneira melhor de olhá-lo é, o arquivo *pode* ser enviada para que a transferência de arquivo pela rede arquive a análise *se for necessário*. Contudo, se o arquivo não é exigido então o arquivo não é enviado.

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`
Para "2," que este é um restrito “não envie” o arquivo para a transferência de arquivo pela rede. Esta ação é final e decisiva, e o processamento da análise do arquivo é feito.

Cenários de exemplo

Esta seção descreve os cenários possíveis em que os arquivos são transferidos arquivos pela rede para a análise corretamente ou não são transferido arquivos pela rede devido a uma razão específica.

Arquivo transferido arquivos pela rede para a análise

AsyncOS mais velho:

Este exemplo mostra um arquivo DOCX que encontre os critérios e seja etiquetado com o **upload_action = 1.** Na linha seguinte, o **arquivo transferido arquivos pela rede para o** Secure Hash Algorithm (SHA) da **análise** é gravado ao log AMP também.

```
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 avante:

Este exemplo mostra um arquivo PPTX que encontre os critérios e seja etiquetado com o **upload_action = recomendado enviar o arquivo para a análise**. Na linha seguinte, o **arquivo transferido arquivos pela rede para o** Secure Hash Algorithm (SHA) da **análise** é gravado ao log AMP também.

```
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
```

Arquivo não transferido arquivos pela rede para a análise porque o arquivo é sabido já

AsyncOS mais velho:

Este exemplo mostra um arquivo PDF que seja feito a varredura pelo AMP com o **upload_action = 2** adicionados ao log da reputação do arquivo. Este arquivo já é sabido à nuvem e não exigido para ser transferido arquivos pela rede para a análise, assim que não é transferida arquivos pela rede outra vez.

```
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 avante:

Este exemplo mostra que o arquivo de amp_watchdog.txt com ampère entra o nível de debug que combina o **upload_action = recomendado não enviar o arquivo para a análise** adicionada ao log da reputação do arquivo. Este arquivo já é sabido à nuvem e não exigido para ser transferido arquivos pela rede para a análise, assim que não é transferida arquivos pela rede outra vez.

```
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
```

Transferência de arquivo pela rede da análise do arquivo de registro através dos encabeçamentos do email

Do CLI, com a opção usando o **logconfig do** comando, a subopção dos **logheaders** pode ser selecionada para alistar e registrar os encabeçamentos dos email processados com o ESA. Usar-se “X-Ampère-Arquivo-transferiu arquivos pela rede” o encabeçamento, um arquivo é transferido arquivos pela rede a qualquer momento ou não transferido arquivos pela rede para a análise do arquivo será gravado aos logs do correio do ESA.

Olhando os logs do correio, resultados para os arquivos transferidos arquivos pela rede para a

análise:

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

Olhando os logs do correio, resultados para os arquivos não transferidos arquivos pela rede para a análise:

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

Informações Relacionadas

- Guias do Usuário de AsyncOS
- Critérios do arquivo para serviços de proteção avançados do malware para produtos de segurança do índice de Cisco
- Teste avançado da proteção do malware ESA (AMP)
- Suporte Técnico e Documentação - Cisco Systems