Filtros do índice ESA para mensagens de Email com acessórios múltiplos

Índice

Introdução

Este documento descreve como as condições satisfeitas negativas do filtro trabalham para os mensagens de Email que contêm acessórios múltiplos na ferramenta de segurança do email de Cisco (ESA).

Problema

Você usa um filtro satisfeito que permita determinados tipos de anexos de Email, quando outros tipos de acessórios deverem ser marcados para a quarentena. Quando um mensagem de Email chega que tenha acessórios múltiplos, um que deve ser permitido e outro que deve ser marcado para a quarentena, o filtro identifica o mensagem completa como *reservado*.

Está aqui o filtro satisfeito que é usado:

```
if attachment filename != (list of attachments), then quarantine
```

Estas funções da circunstância e da ação como pretendidas se o mensagem de Email tem um único acessório, mas ele não funcionam corretamente para as mensagens que contêm acessórios múltiplos, diferentes.

Cenário de exemplo

Estes são os tipos de acessórios que são permitidos:

- rar
- pdf
- jpg

Todos acessórios restantes devem ser enviados para quarantine, como especificado pela

condição e pela ação do filtro.

Condição do filtro

Está aqui a condição do filtro que é usada:

```
if attachment filename != (rar|pdf|jpg)
```

Ação do filtro

Está aqui a ação do filtro que é usada:

```
quarantine
```

A expectativa é tipicamente que se o mensagem de Email contém um acessório **pdf** e um acessório do **txt**, a seguir deve ser quarantined devido ao acessório do **txt** porque não está na lista de acessórios permitidos. Contudo, este filtro satisfeito não funciona como pretendido porque combina o acessório **pdf na** mensagem e o permite diretamente, mesmo que tenha um acessório do **txt**.

Solução

Não é possível quarantine por estas razões o email com o acessório do **txt**:

- As condições do acessório são para **todos os** acessórios que são incluídos em uma mensagem.
- O negativo**! = a** comparação verifica se **alguns dos** acessórios combinam.

Como descrito, se **alguns dos** acessórios são permitidos, como quando combinarem**! =**, o mensagem completa é tratado então como *reservado*. Não há nenhuma maneira em torno deste; é simplesmente a maneira que estas circunstâncias trabalham.

A única outra solução é inverter a lógica e obstruir acessórios específicos, não apenas todo o acessório que não estiver branco-listado.