ESA - Utilizzo di un filtro messaggi per eseguire azioni su messaggi di grandi dimensioni senza allegati

Sommario

[Introduzione](#)
[Requisiti](#)
[Creazione del filtro messaggi](#)
[Applicazione del filtro messaggi all'ESA](#)
[Risorse aggiuntive](#)

Introduzione

Èpossibile che alcuni spammer inviino messaggi molto grandi senza allegati per superare la scansione antispam. Se è possibile inviare un messaggio di dimensioni maggiori rispetto alle dimensioni massime di scansione del modulo antispam dell'ESA, la scansione verrà ignorata. Al momento della scrittura di questo articolo, si consiglia di non aumentare le dimensioni massime della scansione antispam oltre 2 MB, a meno che non sia altrimenti consigliato. Per questo motivo, nella maggior parte dei casi i messaggi di dimensioni superiori a 2 MB possono ignorare facilmente l'antispam.

In questo articolo viene illustrato un concetto per l'esecuzione di azioni su questi tipi di messaggi utilizzando un filtro messaggi.

Requisiti

1. Accesso da riga di comando a Email Security Appliance (ESA).
2. Conoscenze base di come scrivere filtri messaggi.
3. Conoscenze base di Espressione regolare (RegEx).

Creazione del filtro messaggi

In questa sezione verrà creato il filtro messaggi. Questo filtro messaggi consente di trovare tutti i messaggi di dimensioni superiori a 2 MB che non contengono allegati:

1. Aprire un editor di testo e copiare/incollare il seguente filtro messaggi:

```
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
}
```

Nota: *Affinché il filtro messaggi funzioni correttamente, è necessario creare una quarantena di tipo criteri, virus ed epidemie (PVO) corrispondente al nome della quarantena utilizzata*

nell'operazione di quarantena del filtro messaggi. In caso contrario, è necessario utilizzare un tipo di azione diverso. Dopo aver creato la quarantena PVO e aver applicato il filtro messaggi all'ESA, si consiglia di monitorare la quarantena PVO e di rilasciare o eliminare i messaggi in quarantena, se necessario.

2. Da qui è possibile modificare il filtro messaggi per adattarlo alle proprie esigenze specifiche. Ad esempio, se le dimensioni massime della scansione per l'antispam sono impostate su 1 MB, è possibile ridurre le dimensioni del corpo del messaggio a 1 MB.
3. Èinoltre possibile applicare questo filtro ai messaggi solo ai messaggi provenienti da un determinato gruppo di mittenti o listener. Di seguito sono riportati altri due esempi che possono essere utilizzati per gli scopi specificati:

```
large_spam_no_attachment:
if (recv-listener == "IncomingMail") AND ((body-size > 2097152) AND NOT (attachment-size >
0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
}

large_spam_no_attachment:
if (sendergroup != "RELAYLIST") AND ((body-size > 2097152) AND NOT (attachment-size > 0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
}
```

4. Se si desidera apportare ulteriori modifiche, si consiglia di rivedere la sezione relativa al filtro dei messaggi nella Guida all'uso finale dell'ESA. Nella guida sono disponibili sezioni che forniscono un elenco di condizioni e azioni utilizzabili.

Applicazione del filtro messaggi all'ESA

In questa sezione applicheremo all'ESA il filtro messaggi creato nella sezione precedente. I filtri messaggi possono essere applicati solo all'ESA tramite riga di comando. Pertanto, sarà necessario accedere all'ESA dalla riga di comando.

1. Accedere all'ESA dalla riga di comando.
2. Eseguire i seguenti comandi evidenziati per applicare il filtro messaggi all'ESA:

```
ironport.example.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW

Enter filter script.  Enter '.' on its own line to end.
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
} .
1 filters added.
```

3. Da qui è possibile visualizzare il filtro messaggi e verificare che sia attivo e valido. A tale scopo, eseguire i comandi seguenti:

```
ironport.example.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> LIST

Num Active Valid Name
  1   Y      Y   large_spam_no_attachment


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> DETAIL

Enter the filter name, number, or range:
[]> 1

Num Active Valid Name
  1   Y      Y   large_spam_no_attachment
large_spam_no_attachment: if (body-size > 2097152) AND NOT (attachment-size > 0)) {
                              quarantine("large_spam");
                              log-entry("*****This is a large message with no
attachments*****");
                          }
```

4. Eseguire il comando commit e aggiungere eventuali commenti di commit:

```
ironport.example.com> commit

Please enter some comments describing your changes:
[]> Applied large_spam_no_attachment message filter
```

Risorse aggiuntive

[Guida per l'utente finale ESA]