ESA - Gebruik van een berichtfilter om actie te ondernemen tegen grote berichten zonder bijlagen

Inhoud

Inleiding

Mogelijk ziet u dat bepaalde spammers zeer grote berichten zonder bijlagen verzenden, zodat er minder antispammers gescand kunnen worden. Als u een bericht kunt verzenden dat groter is dan het maximale scanformaat van het ESR-antispamprogramma, wordt het scannen van antispam voor dat bericht overgeslagen. Ten tijde van het schrijven van dit artikel raden we niet aan om de maximale scangrootte van anti-spam te verhogen van meer dan 2 MB, tenzij anders aanbevolen. Daarom kunnen boodschappen van meer dan 2 MB in omvang in de meeste gevallen het antispam gemakkelijk omzeilen.

In dit artikel wordt één concept uitgelegd om actie te ondernemen tegen dit soort berichten door gebruik te maken van een berichtfilter.

Vereisten

1. Toegang tot de opdrachtregel tot de e-mail security applicatie (ESA).
2. Basiskennis van het schrijven van berichtfilters.
3. Basiskennis van reguliere expressie (RegEx).

Het berichtfilter maken

In dit deel gaan we het berichtfilter maken. Dit berichtfilter komt overeen met alle berichten die groter dan 2 MB zijn en geen bijlage bevatten:

1. Open een teksteditor en kopieer/plak het volgende berichtfilter:

```
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*****");
}
```

   Opmerking: *U moet een quarantainevoorziening voor beleid, virussen en uitbraak (PVO) maken die overeenkomt met de naam van de quarantaine die wordt gebruikt in de*

quarantaineactie van het berichtfilter, zodat het berichtfilter naar behoren kan functioneren. Anders moet u een ander actietype gebruiken. Als deze PVO-quarantaine is gecreëerd en het berichtfilter op de ESA wordt toegepast, raden we u sterk aan om de PVO-quarantaine te controleren en indien nodig de quarantaineberichten vrij te geven of te verwijderen.

2. Vanaf hier kunt u dit berichtfilter mogelijk aanpassen aan uw specifieke vereisten. Als de maximale scangrootte van uw antispam bijvoorbeeld is ingesteld op 1 MB, kunt u de lichaamsgrootte beperken tot 1 MB.
3. U kunt ook willen dat dit berichtfilter alleen van toepassing is op berichten van een bepaalde sendergroep of luisteraar. Hieronder volgen twee extra voorbeelden die voor uw doeleinden kunnen werken:

```
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. Als u extra wijzigingen wilt aanbrengen, raadt u aan het gedeelte van het bericht van het filter in de ESR-eindgebruikershandleiding te herzien. Er zijn delen in de gids die een lijst bevatten van voorwaarden en acties die kunnen worden gebruikt.

Pas het berichtfilter op de ESA toe

In dit deel passen we het in de voorgaande paragraaf gemaakte berichtenfilter toe op het ESR. Berichtfilters kunnen alleen via de opdrachtregel op de ESA worden toegepast. U hebt dus toegang nodig tot de ESA.

1. Log in op de ESA via opdrachtregel.
2. Start de volgende gemarkeerde opdrachten om het berichtfilter op de ESA toe te passen:

```
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. Vanaf hier kunt u het berichtfilter bekijken en er zeker van zijn dat het actief en geldig is. U kunt dit doen door de volgende opdrachten te gebruiken:

```
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. Start de opdracht Toegeven en voeg eventuele opmerkingen toe die van belang zijn:

```
ironport.example.com> commit

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

Aanvullende bronnen

[ESA-eindgebruikershandleiding]