ESA - Using a message filter to take action on large messages with no attachments

Contents

Introduction

You may find that certain spammers will send very large messages with no attachments in them in order to get past antispam scanning. If they can send a message that is larger than the antispam max scanning size of the ESA antispam engine, antispam scanning will be skipped for that message. As of writing this article, we do not recommend increasing the antispam max scanning size above 2MB unless otherwise recommended. Because of that, messages above 2MB in size can easily bypass antispam in most cases.

This article will explain one concept to take action on these types of messages by utilizing a message filter.

Requirements

1. Command line access to the Email Security Appliance (ESA).
2. Basic knowledge of how to write message filters.
3. Basic knowledge of Regular Expression (RegEx).

Creating the message filter

In this section, we are going to create the message filter. This message filter will match all messages that are over 2MB in size and don't contain an attachment:

1. Open a text editor and copy/paste the following message filter:

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

Note: *You will need to create a Policy, Virus and Outbreak (PVO) quarantine that matches the name of the quarantine used in the quarantine action of the message filter in order for the message filter to function as is. Otherwise, you must use a different action type. Once this PVO quarantine is created and the message filter is applied to the ESA, we strongly recommend that you monitor the PVO quarantine and release or delete quarantined*

messages as necessary.

2. From here, you may want to alter this message filter to fit your specific requirements. For example, if your antispam max scanning size is set to 1MB, you can reduce the body-size down to 1MB.
3. You may also want this message filter to only apply to messages from a particular sendergroup or listener. The following are two additional examples that could work for your purposes:

```
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. If you want to make any additional changes, I'd recommend reviewing the message filter section in the ESA End-Use Guide. There are sections in the guide that provide a list of conditions and actions that can be used.

Apply the message filter to the ESA

In this section, we are going to apply the message filter created in the previous section to the ESA. Message filters can only be applied to the ESA via command line. So, you will need command line access to the ESA.

1. Log into the ESA via command line.
2. Run the following highlighted commands to apply the message filter to the 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. From here, you may want to view the message filter and ensure it's active and valid. You can do that by running the following commands:

```
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. Run the commit command and add any relevant commit comments:

```
ironport.example.com> commit

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

Additional resources

[ESA End-User Guide]