ESA -使用消息过滤器采取对大消息的行动没有附件

Contents

Introduction

您可以发现某些犯规推销者将传送非常大信息没有在他们的附件为了通过antispam扫描。如果他们能传送大于ESA antispam引擎的antispam最大扫描大小的信息， antispam扫描为该消息将被跳过。自写作此条款，我们不推荐增加antispam最大扫描大小高于2MB，除非推荐。因此，消息高于2MB能在许多情况下容易地在大小上绕过antispam。

此条款将说明一个概念通过使用消息过滤器采取对这些消息类型的行动。

Requirements

1. 对电子邮件安全工具(ESA)的Line命令访问。
2. 基础知识如何写消息过滤器。
3. 基础知识常规表示(REGEX)。

创建消息过滤器

在此部分，我们创建消息过滤器。此消息过滤器将匹配在大小上在2MB的所有消息和不包含附件：

1. 打开文本编辑并且复制/粘贴下列信息过滤器：

```
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:*您将需要创建匹配检疫的名字使用在消息过滤器检疫动作为了消息过滤器能作用的策略、病毒和爆发(PVO)检疫和。否则，您必须使用一不同的操作类型。一旦此PVO检疫被创建，并且消息过滤器被应用于ESA，我们强烈建议您监控PVO检疫并且如所需要发布或者删除被检疫的消息。*
2. 从这里，您可以要修改此消息过滤器适合您的特定需求。例如，如果您的antispam最大扫描大小设置为1MB，您可以使正文大小降低下来到1MB。
3. 您可以也此消息过滤器只适用于消息从特定的sendergroup或监听程序。下列是可能为您的目的工作的两个另外的示例：

```
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. 如果要做任何另外的变动，我会推荐查看在ESA最终用途指南的消息过滤器部分。有提供情况和动作列表能使用在指南的部分。

应用消息过滤器于ESA

在此部分，我们应用在前面的部分创建的消息过滤器于ESA。消息过滤器可能只被应用于ESA通过line命令。因此，您将需要对ESA的line命令访问。

1. 日志到ESA里通过line命令。
2. 运行以下突出显示的命令应用消息过滤器于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. 从这里，您可以要查看消息过滤器，并且保证它是活跃和有效的。您能通过运行以下命令执行那：

```
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. 运行commit命令并且添加所有相关进行备注：

```
ironport.example.com> commit

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

附加资源

[ESA终端用户指南]