如何识别和解决 ESA 上的邮件循环状况？

Contents

Introduction

本文档介绍如何识别邮件安全设备 (ESA) 上的邮件循环。

背景信息

如有注入超过 3 次且具有相同邮件 ID 的邮件，则表示存在邮件循环。邮件循环会导致出现高 CPU 使用率、传送缓慢和整体性能问题等症状。通常邮件 ID 注入不止一次即表示出现循环，但有时它们是因为出现问题而注入不止一次，或者是粗心的垃圾邮件发送者不断注入具有相同邮件 ID 的同一封垃圾邮件。

更具代表性的邮件循环是由于邮件基础设施问题而导致，在您的网络中从一个邮件服务器到另一个邮件服务器不断地发送相同的邮件或一组邮件。 这些邮件会按这种方式发送很长一段时间，这不是一件好事，这不仅会占用您的网络带宽，而且还会招致 ESA 处理成本。

解决方案

如果您怀疑出现这种问题，识别邮件循环通常会很容易，但您需要盯着它。
登录系统的命令行界面 (CLI) 并发出以下命令之一，如果您认为需要，也可以执行这两个命令：

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

特别适合搜索邮件 ID，如果您看到反复出现完全相同的 ID，则您知道出现了邮件循环。 但是，有时候这还不够，因为其中一个邮件服务器集合相同的邮件可能有助于更改或删除邮件 ID 报头。 因此，如果您利用邮件 ID 检查没有识别出任何循环，请继续尝试主题检查。

假设您设法通过邮件 ID 来找到循环邮件，您也会想找出关于邮件及其父连接 (ICID) 的其他信息。
在同一个日志行中给出邮件 ID 和 MID，您可执行：

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

给出结果输出，您可找到相关 ICID 和 DCID 并执行：

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

现在您应该拥有完整的连接（邮件事务），并可看到邮件来自何处以及要传送到何处（如果已发生）。识别循环邮件后，下一步是查看邮件，以便您可解决问题。 如果没有消除产生循环的原因，则很可能此邮件和其他邮件将继续循环发送或问题很快将再次出现。

创建一个与以下类似的邮件过滤器：

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

现在提交更改并发出此命令以检查邮件：

```
tail looper
```

利用查看邮件日志所获得的远程系统信息，以及查看邮件本身所获得的其他信息，您应该能够确定问题所在。

如何防止发生邮件循环？

在复杂环境中，要防止发生循环会很困难 - 关键是了解邮件如何流入您的环境，以及在 ESA 或另一个设备上发生的新网络变化如何影响该流量。出现失控邮件循环的一个常见原因是删除了 Received 报头。 ESA 将自动检测，并在看到邮件中有 100 个 Received 报头时停止邮件循环，但 ESA 会允许删除此报头，这通常会导致出现严重的邮件循环。 除非有*真正*充足的理由，请勿关闭 Received 报头，否则会导致报头被删除。

以下是可帮助防止或修复邮件循环的过滤器示例：

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
 if (header("X-ExtLoopCount2")) {
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
                  $RemoteIP");}}
           else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
         else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
       else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
     else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
   else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
 else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```