ESA詐騙郵件過濾

目錄

簡介

本檔案介紹垃圾郵件和欺詐性電子郵件進入網路時，思科電子郵件安全裝置(ESA)遇到的問題。

問題

欺詐者試圖類比電子郵件。當電子郵件模擬貴公司的一名員工（聲稱來自該員工）時，它可能特別具有欺騙性，並可能導致混淆。為了解決此問題，電子郵件管理員可能會嘗試阻止似乎來自公司內部的入站郵件(偽*裝郵*件)。

從域名中含有公司返回地址的Internet阻止入站郵件，似乎符合邏輯，這樣可以解決問題。遺憾的是，當您以這種方式阻止郵件時，它還可以同時阻止合法電子郵件。請考慮以下示例：

- 員工旅行並使用一家酒店Internet服務提供商(ISP)，該服務提供商透明地將所有簡單郵件傳輸協定(SMTP)流量重定向到ISP郵件伺服器。傳送郵件時，郵件似乎直接流經企業SMTP伺服器，但在將郵件傳送到企業之前，實際上是通過第三方SMTP伺服器傳送的。

- 員工訂閱電子郵件討論清單。當郵件傳送到電子郵件清單時，會將其返回給所有訂戶，顯然是從始發者傳送的。

- 外部系統用於監控外部可見裝置的效能或可達性。出現警報時，該電子郵件在返回地址中包含公司域名。WebEx等第三方服務提供商經常這樣做。

- 由於臨時網路配置錯誤，來自公司內部的郵件將通過入站偵聽程式而不是出站偵聽程式傳送。

- 公司外部人員收到一封郵件，郵件使用者代理(MUA)將郵件轉發回公司，該代理使用新的標題行而不是原始標題。

- 基於Internet的應用程式(如Federal Express **shipping頁**或Yahoo **email this article** page)會建立帶有返回地址並指向公司的合法郵件。 郵件是合法的，其源地址來自公司內部，但並非源自公司內部。

這些示例顯示，如果根據域資訊阻止入站郵件，可能會導致誤報。

解決方案

本節介紹為了解決此問題，您應該執行的建議操作。

套用篩選條件

為了避免丟失合法電子郵件，請不要根據域資訊阻止入站郵件。相反，您可以在這些型別的郵件進入網路時標籤其主題行，這向收件人指示這些郵件可能是偽造的。這可以通過郵件篩選器或內容篩選器來實現。

這些過濾器的基本策略是檢查向後指向的正文標題行(From資料是最重要的)，以及RFC 821信封發件人。這些標題行最常顯示在MUA中，並且是最可能由欺詐人員偽造的標題行。

下一個示例中的郵件過濾器顯示如何標籤可能模擬的郵件。此過濾器執行多個操作：

- 如果主題行中已**有「{可能偽造}」**，則篩選器不會新增其他副本。當回覆包含在消息流中並且主題行可能在消息執行緒完成之前多次通過郵件網關時，這一點非常重要。

- 此過濾器搜尋以域名@yourdomain.com結尾的地址的信封發件人或From信頭。必須注意的是，發件人搜尋會自動不區分大小寫，但發件人標*頭搜*索不區分大小寫。如果在任一位置找到域名，則篩選器將在主題行的末尾插入「{Possible Forged}」。

以下是篩選器的範例：

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com")
       {
           strip-header("Subject");
           insert-header("Subject", "$Subject {Possibly Forged}");
       }
   }
```

附加措施

由於沒有簡單的方法來識別合法郵件中的欺騙郵件，因此沒有方法完全消除此問題。因此，思科建議您啟用IronPort反垃圾郵件掃描(IPAS)，從而有效識別欺詐郵件（網路釣魚）或垃圾郵件並積極阻止它。此反垃圾郵件掃描程式的使用與上一節中描述的過濾器結合使用時，可在不丟失合法電子郵件的情況下提供最佳結果。

如果您必須識別進入網路的欺詐性電子郵件，則應考慮使用域金鑰識別郵件(DKIM)技術；它需要更多設定，但這是針對網路釣魚和欺詐性電子郵件的有效措施。

> **附註**：有關郵件過濾器的詳細資訊，請參閱思科郵件安全裝置支援頁面上的AsyncOS使用手冊。