排除來自受感染帳戶的ESA上不需要的出站電子郵件故障

目錄

簡介

本文描述如何在內部使用者帳戶受到攻擊並全域性傳送未經授權的電子郵件時，對郵件安全裝置(ESA)上的隊列進行故障排除和糾正。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於ESA的AsyncOS 7.6及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

疑難排解

如果已知傳送垃圾郵件的帳戶，建議鎖定該帳戶；否則，一旦通過ESA上的調查發現該帳戶，建議鎖定該帳戶。

工作隊列檢查

當工作隊列計數器中有大量電子郵件且進入系統的電子郵件速率遠遠超過退出系統的速率時，這表明對工作隊列存在影響。可以使用workqueue命令執行檢查。

```
C370.lab> workqueue status

Status as of:  Thu Feb 06 12:48:02 2014 GMT
Status:        Operational
Messages:      48654

C370.lab> workqueue rate 5

Type Ctrl-C to return to the main prompt.

Time      Pending    In   Out
12:48:04    48654    48     2
12:48:09    48700    31     0
```

工作隊列中的電子郵件發件人或主題已知

為了刪除影響工作隊列的電子郵件，建議使用郵件過濾器。使用郵件過濾器將允許ESA在工作隊列的開頭而不是結尾處理這些郵件，以便以更有效的時間間隔幫助刪除郵件。

此過濾器可用於實現以下目標：

```
C370.lab> 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.
[]> new

Enter filter script.  Enter '.' on its own line to end.

FilterName:
if (mail-from == 'abc@abc1.com')
{
drop();
}
.

OR

FilterName:
if (subject == "^SUBJECT NAME$")
{
drop();
}
.
```

傳遞隊列檢查

tophosts命令將顯示當前受影響的主機。在即時環境中，您將看到收件人主機（當前活動傳遞隊列

）受大量活動收件人的影響。對於此輸出，示例為impactedhost.queue。

```
C370.lab> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>  1

Status as of:                  Thu Feb 06 12:52:17 2014 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out     Recip.    Bounced    Bounced

1   impactedhost.queue          321550     50        440      75568       8984
2   the.euq.queue                    0      0          0          0          0
3   the.euq.release.queue            0      0          0          0          0
```

如果受影響主機是一個不熟悉的收件人域（在刪除所有電子郵件之前需要瞭解詳細資訊），可以使用showreceipents、show message和deleterecipients命令。showreceients命令將顯示郵件的郵件ID(MID)、郵件大小、傳送嘗試、信封發件人、信封收件人和主題。

```
C370.lab> showrecipients

Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to show.
> impactedhost.queue
```

如果傳遞隊列中的疑似MID看起來合法，您可以在採取任何操作之前使用show message命令來顯示消息源。

```
C370.lab> showmessage

Enter the MID to show.
[]>
```

一旦確認為垃圾郵件，若要刪除這些電子郵件，請繼續並使用deleterecipient命令。該命令將提供三個選項，用於刪除傳送隊列中的電子郵件；按信封發件人、按收件人主機或傳送隊列中的所有電子郵件。

```
C370.lab> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2

Please enter the Envelope From address for the messages you wish to delete.
```

```
[]>
```

主動監控和操作

在ESA上的9.0+ AsyncOS版本中，可以使用名為Header Repeats Rule的新消息過濾條件。

報頭重複規則

如果在給定時間點，指定數量的郵件為：

- 最近一小時內偵測到的是同一個主題
- 在過去一小時內檢測到來自同一信封的發件人。
- header-repeats(<target>, <threshold> [, <direction>])

有關此條件的詳細資訊，請參閱裝置的聯機幫助指南。

登入到CLI並部署篩選器，以便運行所需的檢查和操作。示例篩選器用於在達到閾值後刪除電子郵件或通知管理員。

```
C370.lab> 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.
[]> new

Enter filter script.  Enter '.' on its own line to end.

FilterName:
if header-repeats('mail-from',1000,'outgoing')
{
drop();
}
.

OR

FilterName:
if header-repeats('subject',1000,'outgoing')
{
notify('admin@xyz.com');
}
.
```

相關資訊

- [ESA常見問題：如何手動清除電子郵件隊列中的收件人？]

- 技術支援與文件 - Cisco Systems