機密が漏洩した アカウントからの ESA の不必要な送信メールを解決して下さい

目次

概要

内部ユーザ ユーザー アカウントがおよび送信された unsoliticited メール グローバルに妥協されたことこの資料にイベントの E メール セキュリティ アプライアンス (ESA) のキューを解決し訂正する方法を記述されています。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

この 文書に記載されている 情報は ESA のための AsyncOS 7.6 およびそれ以降に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

トラブルシューティング

知られていれば一度 ESA の調査によって検出されるアカウントの下でスパムを、他では口ックする送信 するアカウントの下で口ックすることは賢明です。

Workqueue チェック

workqueue カウンターの多数のメールあるおよび入力するメールのレートがシステムずっとシステムを終了するレートを超過するとき、これは workqueue に影響があることを示します。 チェックを行う workqueue コマンドを使用できます。

```
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
```

Workqueue のメールの送信側かサブジェクトは知られています

workqueue に影響を与えるメールを取除くために、メッセージ フィルターの使用は推奨されます。 メッセージ フィルターの使用方法は端よりもむしろ workqueue の始めに操作に効率的間隔のメールの削除と助けるために ESA にこれらのメールを与えます。

このフィルタがこれを実現させるのに使用することができます:

```
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();
}
.
```

配信キュー チェック

tophosts コマンドは現在によって影響を与えられたホストを示したものです。 ライブ環境で受信者のホスト（現在のアクティブな配信キュー）が多数のアクティブな受信者と影響を与えられることを見ます。 この出力に関しては、例は impactedhost.queue です。

```
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
```

もし影響を与えられたホストがより詳しい 情報がすべてのメールの削除の前に必要となる不慣れな受信者のドメインなら、コマンド showreceipients、showmessage および deleterecipients は使用することができます。 showreceipients コマンドはメッセージID （MID）、メールのメッセージサイズ、配信試行、エンベロープ送信側、エンベロープ受信者およびサブジェクトを表示したものです。

```
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
```

配信キューの疑われた MID が正規に検知 すれば、処置をとる前にメッセージ ソースを表示するために showmessage コマンドを使用できます。

```
C370.lab> showmessage

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

これらのメールを取除くために、スパムとして確認されて続行し、deleterecipient コマンドを使用して下さい。 コマンドは配信キューを離れてメール削除に 3 つのオプションを提供したものです; エンベロープ送信側、受信者のホストによって、か配信のすべてのメールによって並べて下さい。

```
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.
[]>
```

プロアクティブな監視および操作

ESA のバージョン 9.0+ AsyncOS で、Header Repeats ルールと呼ばれる新しいメッセージ フィルター状態は利用できます。

ヘッダ リピート ルール

ヘッダ リピート ルールは本当にある特定の時点で、メッセージの指定 番号評価します:

- 同じ事項によって最後の 1 時間に検出されます。
- 同じエンベロープ送信側から最後の 1 時間に検出されます。
- ヘッダ リピート (<target>、<threshold> [、<direction>])

この条件のより詳しい 情報はデバイスのオンライン ヘルプ ガイドで利用できます。

CLI に ログイン し、望まれるこのチェックおよび操作を実行するためにフィルタを展開して下さい。 メールを廃棄するか、またはしきい値の後で admin を知らせるフィルタ例は会います。

```
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');
}
.
```

関連情報

- ESA に関する FAQ： E メール キューから受信者を手動で消去するにはどうしますか。
- テクニカル サポートとドキュメント – Cisco Systems