Risoluzione dei problemi relativi alle e-mail in uscita indesiderate provenienti da account compromessi sull'ESA

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle code su Email Security Appliance (ESA) nel caso in cui un account utente interno sia stato compromesso e invii messaggi di posta elettronica non richiesti a livello globale.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è AsyncOS 7.6 e versioni successive per ESA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Risoluzione dei problemi

Èconsigliabile bloccare l'account che invia lo spam se è noto, altrimenti bloccare l'account una volta scoperto tramite l'indagine sull'ESA.

Controlli coda di lavoro

Quando il contatore della coda di lavoro contiene un numero elevato di messaggi di posta elettronica e la frequenza dei messaggi che entrano nel sistema supera di gran lunga la frequenza con cui escono dal sistema, ciò indica che c'è un impatto sulla coda di lavoro. È possibile utilizzare il comando workqueue per eseguire il controllo.

```
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
```

Mittente o oggetto dei messaggi di posta elettronica nella coda di lavoro noto

Per rimuovere i messaggi di posta elettronica che influiscono sulla coda di lavoro, è consigliabile utilizzare un filtro messaggi. L'uso di un filtro messaggi consentirà all'ESA di agire su questi messaggi all'inizio della coda di lavoro piuttosto che alla fine per assistere con la rimozione dei messaggi e-mail ad un intervallo più efficiente.

Questo filtro può essere utilizzato per ottenere quanto segue:

```
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();
}
.
```

Controllo coda di recapito

Il comando **tophosts** visualizzerà gli host interessati. In un ambiente live, l'host del destinatario (coda di recapito attiva corrente) sarà interessato da un numero elevato di destinatari attivi. Per questo output, l'esempio è **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
```

Se l'host interessato è un dominio del destinatario sconosciuto in cui sono necessarie ulteriori informazioni prima della rimozione di tutti i messaggi di posta elettronica, è possibile utilizzare i comandi **show receivipients**, **show message** e **deleteterecipients**. Il comando **show receivipients** visualizza l'ID messaggio (MID), le dimensioni del messaggio, i tentativi di recapito, il mittente della busta, i destinatari della busta e l'oggetto dell'e-mail.

```
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
```

Se il MID sospetto nella coda di recapito sembra legittimo, è possibile utilizzare il comando **show message** per visualizzare l'origine del messaggio prima di eseguire qualsiasi operazione.

```
C370.lab> showmessage

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

Una volta confermato che si tratta di posta indesiderata, per rimuovere queste e-mail procedere e usare il comando **deletecipient**. Il comando fornisce tre opzioni per l'eliminazione dei messaggi e-mail dalla coda di recapito; Per mittente busta, Per host destinatario o Tutti i messaggi di posta elettronica nella coda di recapito.

```
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.
[]>
```

Monitoraggio e azioni proattive

Nella versione 9.0+ AsyncOS sull'ESA, è disponibile una nuova condizione del filtro messaggi chiamata Header Repeats Rule.

Regola ripetizioni intestazione

La regola Ripeti intestazione restituisce true se in un determinato momento viene restituito un numero specificato di messaggi:

- Con lo stesso soggetto vengono rilevati nell'ultima ora.
- Dallo stesso mittente della busta sono stati rilevati nell'ultima ora.
- header-repeat(<destinazione>, <soglia> [, <direzione>])

Ulteriori informazioni su questa condizione sono disponibili nella Guida in linea del dispositivo.

Accedere alla CLI e distribuire il filtro per eseguire questo controllo e l'azione desiderata. Un filtro di esempio per eliminare i messaggi di posta elettronica o notificare a un amministratore quando viene raggiunta una soglia.

```
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');
}
.
```

Informazioni correlate

- Domande frequenti ESA: Come si cancellano manualmente i destinatari dalla coda di posta elettronica?
- Documentazione e supporto tecnico – Cisco Systems