Correos electrónicos salientes indeseados del Troubleshooting en el ESA de las cuentas comprometidas

Contenido

Introducción

Este documento describe cómo resolver problemas y corregir las colas de administración del tráfico en el dispositivo de seguridad del correo electrónico (ESA) en un evento que una cuenta de usuario interno se ha comprometido y los correos electrónicos unsoliticited enviados global.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en AsyncOS 7.6 y posterior para el ESA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Troubleshooting

Es recomendable bloquear abajo de la cuenta que envía el Spam si se sabe, si no bloquea abajo de la cuenta descubierta una vez vía la investigación en el ESA.

Controles de Workqueue

Cuando hay un gran número de email en el contador del workqueue y el índice de email que ingresen el sistema excede lejos la tarifa que sale el sistema, ésta indica que hay un impacto en el workqueue. Usted puede utilizar el comando del workqueue de realizar el control.

```
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
```

Conocen al remitente o al tema de los correos electrónicos en el Workqueue

Para quitar los correos electrónicos que afectan el workqueue, el uso de un filtro del mensaje se recomienda. El uso de un filtro del mensaje no prohibirá a ESA a la acción estos correos electrónicos al principio del workqueue bastante que el extremo para ayudar con el retiro de los correos electrónicos en un intervalo más eficiente.

Este filtro se puede utilizar para alcanzar esto:

```
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();
}
.
```

Control de la cola de la salida

El comando de los **tophosts** mostrará los host afectados corriente. En un entorno vivo usted verá que el host receptor (cola activa actual de la salida) será afectado con un gran número de beneficiario activo. Para esta salida, el ejemplo es **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
```

Si el host afectado es un dominio receptor desconocido donde la Más información se requiere antes del retiro de todos los correos electrónicos, los **showreceipients**, el **showmessage**, y los **deleterecipients de los** comandos pueden ser utilizados. El comando de los **showreceipients** visualizará el ID del mensaje (MEDIADOS DE), el tamaño del mensaje, las tentativas de la salida, el remitente del sobre, los beneficiarios del sobre, y al tema del correo electrónico.

```
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
```

En caso que el MEDIADOS DE sospechoso en la cola de la salida parezca legítimo, usted puede utilizar el comando del **showmessage** para visualizar el Origen de los mensajes antes de que usted tome cualquier medidas.

```
C370.lab> showmessage

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

Confirmado una vez como Spam, para quitar estos correos electrónicos, proceda y utilice el comando **deleterecipient**. El comando proporcionará tres opciones para la cancelacíon del correo electrónico de la cola de la salida; Por el remitente del sobre, por el host receptor, o todos los correos electrónicos en la salida haga cola.

```
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.
[]>
```

Control proactivo y acción

En la versión 9.0+ AsyncOS en el ESA, nueva una regla llamada de Header Repeats del filtro del mensaje condición está disponible.

La encabezado relanza la regla

La regla de las repeticiones de la encabezado evalúa para verdad si en una punta dada a tiempo, un número especificado de mensajes:

- Con el mismo tema se detectan sobre la una hora más pasada.
- Del mismo remitente del sobre se detectan sobre la una hora más pasada.
- encabezado-repeticiones (<target>, [, <direction>] del <threshold>)

La Más información en esta condición está disponible en la guía de la Ayuda en Línea de su dispositivo.

El registro en el CLI y despliega el filtro para ejecutar este control y acción deseados. Un filtro del ejemplo para caer los correos electrónicos o para notificar un admin después de un umbral se resuelve.

```
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');
}
.
```

Información Relacionada

- ESA FAQ: ¿Cómo hacen yo manualmente los beneficiarios claros de la cola del correo electrónico?
- Soporte Técnico y Documentación - Cisco Systems