

Pesquisa defeitos email de partida indesejáveis no ESA das contas comprometidas

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Troubleshooting](#)

[Verificações de Workqueue](#)

[O remetente ou o assunto dos email no Workqueue são conhecidos](#)

[Verificação da fila da entrega](#)

[Monitoramento pró-ativo e ação](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como pesquisar defeitos e corrigir as filas na ferramenta de segurança do email (ESA) em um evento que uma conta de usuário interno esteve comprometida e email unsolicited mandados globalmente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

A informação neste documento é baseada em AsyncOS 7.6 e mais atrasado para o ESA.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Troubleshooting

É aconselhável travar abaixo da conta que envia o Spam se se sabe, se não trava abaixo da conta descoberta uma vez através da investigação no ESA.

Verificações de Workqueue

Quando há um grande número email no contador do workqueue e a taxa de email que incorporam o sistema excede distante a taxa que retira o sistema, esta indica que há um impacto no workqueue. Você pode usar o comando do workqueue executar a verificação.

```
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

O remetente ou o assunto dos email no Workqueue são conhecidos

A fim remover os email que impactam o workqueue, o uso de um filtro da mensagem é recomendado. O uso de um filtro da mensagem permitirá ao ESA à ação estes email no início do workqueue um pouco do que a extremidade a fim ajudar com a remoção dos email em um intervalo dos mais eficiente.

Este filtro pode ser usado para conseguir isto:

```
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();
}
```

Verificação da fila da entrega

O comando dos **tophosts** mostrará os anfitriões impactados corrente. Em um ambiente vivo você verá que o host destinatário (fila ativa atual da entrega) estará impactado com um grande número receptor ativo. Para esta saída, o exemplo é **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.
```

| # | Recipient Host            | Active Recip. | Conn. Out | Deliv. Recip. | Soft Bounced | Hard Bounced |
|---|---------------------------|---------------|-----------|---------------|--------------|--------------|
| 1 | <b>impactedhost.queue</b> | <b>321550</b> | <b>50</b> | <b>440</b>    | <b>75568</b> | <b>8984</b>  |
| 2 | the.euq.queue             | 0             | 0         | 0             | 0            | 0            |
| 3 | the.euq.release.queue     | 0             | 0         | 0             | 0            | 0            |

Se o host impactado for um domínio destinatário estranho onde a informação adicional esteja exigida antes da remoção de todos os email, os **showrecipients**, o **showmessage**, e os **deleterecipients** dos comandos podem ser usados. O comando dos **showrecipients** indicará o ID de mensagem (MEADOS DE), o tamanho de mensagem, as tentativas da entrega, o remetente do envelope, os receptores do envelope, e o assunto do email.

```
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
```

Caso o MEADOS DE suspeitado na fila da entrega olhar legítimo, você pode usar o comando do **showmessage** a fim indicar o origem de mensagem antes que você tome toda a ação.

```
C370.lab> showmessage
```

```
Enter the MID to show.
```

```
[ ]>
```

Confirmado uma vez como o Spam, a fim remover estes email, continue e use o comando **deleterecipient**. O comando fornecerá três opções para o supressão do email fora da fila da entrega; Por remetente do envelope, pelo host destinatário, ou por todos os email na entrega

enfileire.

```
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.

```
[]>
```

Monitoramento pró-ativo e ação

Na versão 9.0+ AsyncOS no ESA, uma regra chamada de Encabeçamento Repetição do filtro da mensagem condição nova está disponível.

O encabeçamento repete a regra

A regra das repetições do encabeçamento avalia para retificar se em um ponto dado a tempo, um número especificado de mensagens:

- Com o mesmo assunto são detectados na última uma hora.
- Do mesmo remetente do envelope são detectados na última uma hora.
- encabeçamento-repetições (<target>, [, <direction>] do <threshold>)

A informação adicional nesta circunstância está disponível no guia da ajuda online do seu dispositivo.

O log no CLI e distribui o filtro a fim executar estas verificação e ação desejadas. Um filtro do exemplo para deixar cair email ou notificar um admin após um ponto inicial é encontrado.

```
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');  
}  
.
```

Informações Relacionadas

- [ESA FAQ: Como fazem mim manualmente os receptores claros da fila do email?](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)