Probleemoplossing ongevraagde uitgaande e-mails op het ESR op basis van gecomprimeerde rekeningen

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen en hoe u de wachtrijen op e-mail security applicatie (ESA) kunt corrigeren als een interne gebruikersaccount gecompromitteerd is en wereldwijd onverklaarde e-mails verstuurd wordt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op AsyncOS 7.6 en later op ESA.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Problemen oplossen

Geadviseerd wordt de account die de spam verstuurt, te vergrendelen indien deze bekend is, anders de rekening te blokkeren die eenmaal was ontdekt via het onderzoek van de ESA.

Controles van werkvoorraden

Wanneer er een groot aantal e-mails in de werkrijteller staat en het aantal e-mails dat het systeem binnenkomt veel hoger is dan het aantal dat het systeem verlaat, duidt dit erop dat er een impact is op de werkwachtrij. U kunt de werkrijopdracht gebruiken om de controle uit te voeren.

```
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
```

Zender of onderwerp van e-mails in de werkwachtrij staat bekend

Om e-mails te verwijderen die van invloed zijn op de werkwachtrij, wordt het gebruik van een berichtfilter aanbevolen. Met het gebruik van een berichtenfilter kan de ESA deze e-mails aan het begin van de werkwachtrij in plaats van aan het einde activeren om te helpen bij het verwijderen van de e-mails met een efficiënter interval.

Dit filter kan worden gebruikt om dit te bereiken:

```
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();
}
.
```

Controle van leverwachtrij

De opdracht Tophosts toont de huidige getroffen hosts. In een levend milieu zult u de ontvangende gastheer (huidige actieve bestelrij) zien van invloed zijn met een groot aantal actieve ontvanger. Voor deze uitvoer is het voorbeeld **impactedhost.wachtrij**.

```
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
```

Als de impacthost een onbekend ontvankelijk domein is waar verdere informatie nodig is voordat alle e-mails worden verwijderd, kunnen de opdrachten **showontvangers**, **showmessage** en **deleterecients** worden gebruikt. De opdracht van **de** presentatoren toont de BerichtID (MID), berichtgrootte, leveringspogingen, Envelope Sender, Envelope Recipient(s) en het onderwerp van de 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
```

Als de vermoedelijke MID in de bezorgingsrij er legitiem uitziet, kunt u de opdracht showberichten gebruiken om de bron van het bericht weer te geven voordat u enige actie onderneemt.

```
C370.lab> showmessage

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

Nadat dit is bevestigd als spam, kunt u deze e-mails verwijderen door de opdracht verwijderen. De opdracht biedt drie opties voor het per e-mail wissen van de bezorgingswachtrij. Door zender in te sturen, door ontvangende host of alle e-mails in de bezorgingswachtrij.

```
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.
[]>
```

Proactieve bewaking en actie

Op versie 9.0+ AsyncOS op het ESA is er een nieuwe berichtfiltervoorwaarde beschikbaar, genaamd Header Repeats Rule.

Regel voor herhaling van kop

De regel Herhalingen van de Kop evalueert tot ware als op een bepaald punt in tijd een bepaald aantal berichten:

- Met hetzelfde onderwerp wordt in het laatste uur ontdekt.
- Van dezelfde envelopzender wordt in het laatste uur ontdekt.
- header-repeats (<target>, <drempelwaarde> [, <directie>])

Aanvullende informatie over deze aandoening is beschikbaar in de online Help-gids van uw apparaat.

Log in op de CLI en stel het filter in om deze controle en actie te gebruiken. Een voorbeeldfilter om e-mails te laten vallen of om een beheerder te melden nadat een drempel is bereikt.

```
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');
}
.
```

Gerelateerde informatie

- ESA FAQ: Hoe kan ik de ontvangers handmatig uit de e-mailrij ontruimen?
- Technische ondersteuning en documentatie – Cisco Systems