감염된 어카운트에서 ESA에서 원치 않는 아웃바운드 이메일 문제 해결

목차

소개

이 문서에서는 내부 사용자 계정이 감염되어 전역적으로 무결점 이메일을 보낸 경우 ESA(Email Security Appliance)에서 대기열을 트러블슈팅하고 수정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 AsyncOS 7.6 이상 for ESA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제 해결

스팸을 전송하는 어카운트가 알려진 경우 이를 잠그는 것이 좋습니다. 그렇지 않으면 ESA에서 조사를 통해 발견된 어카운트를 잠가 두는 것이 좋습니다.

작업 대기열 검사

작업 대기열 카운터에 많은 전자 메일이 있고 시스템에 들어오는 전자 메일의 비율이 시스템을 종료하는 속도를 훨씬 초과할 경우 작업 대기열에 영향이 있음을 나타냅니다.workqueue 명령을 사용

하여 검사를 수행할 수 있습니다.

```
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
```

작업 대기열의 보낸 사람 또는 전자 메일 제목을 알 수 있음

작업 대기열에 영향을 주는 이메일을 제거하려면 메시지 필터를 사용하는 것이 좋습니다.메시지 필터를 사용하면 ESA는 더 효율적인 간격으로 이메일을 제거하는 데 도움이 되도록 작업 대기열의 시작 부분에 이러한 이메일을 실행할 수 있습니다.

이 필터를 사용하여 다음을 수행할 수 있습니다.

```
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();
}
.
```

배달 큐 확인

tophosts 명령은 현재 영향을 받는 호스트를 표시합니다.라이브 환경에서는 수신자 호스트(현재 활성 배달 대기열)가 많은 활성 수신자의 영향을 받게 됩니다.이 출력의 예는 impactedhost.**queue입니다**.

```
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
```

영향을 받는 호스트가 익숙하지 않은 수신자 도메인이어야 모든 이메일을 제거하기 전에 추가 정보가 필요한 경우 명령**은 수신인**, **showmessage** 및 deleterecipients를 사용할 수 있습니다.show **receifications** 명령은 MID(메시지 ID), 메시지 크기, 배달 시도, 봉투 발신자, 봉투 수신자 및 이메일 제목을 표시합니다.

```
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
```

배달 대기열에서 의심스런 MID가 합법적인 것처럼 보이는 경우 작업을 수행하기 전에 메시지 소스를 표시하기 위해 **showmessage** 명령을 사용할 수 있습니다.

```
C370.lab> showmessage

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

스팸으로 확인되면 이러한 이메일을 제거하려면 deleterecipient 명령을 계속 **사용합니다**.이 명령은 전달 대기열에서 전자 메일을 삭제하는 세 가지 옵션을 제공합니다.Envelope Sender, By Recipient Host 또는 전달 대기열의 모든 이메일입니다.

```
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.
[]>
```

사전 모니터링 및 조치

ESA의 버전 9.0+ AsyncOS에서 Header Repeats Rule이라는 새로운 메시지 필터 조건을 사용할 수 있습니다.

헤더 반복 규칙

지정된 시점에 지정된 수의 메시지가 있는 경우 Header Repeats(헤더 반복) 규칙이 true로 평가됩니다.

- 지난 1시간 동안 동일한 주제와 함께 탐지됩니다.
- 지난 1시간 동안 동일한 봉투 발신자에서 탐지됩니다.
- header-repeats(<target>, <threshold> [, <direction>])

이 조건에 대한 자세한 내용은 디바이스의 온라인 도움말 가이드를 참조하십시오.

CLI에 로그인하여 이 확인 및 원하는 작업을 실행하려면 필터를 배포합니다. 임계값이 충족된 후 전자 메일을 삭제하거나 관리자에게 알리기 위한 예제 필터입니다.

```
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');
}
.
```

관련 정보

- ESA FAQ:이메일 대기열에서 수신자를 수동으로 지우려면 어떻게 합니까?
- 기술 지원 및 문서 – Cisco Systems