ESA에서 메일 루프 상황을 식별하고 해결하려면 어떻게 해야 합니까?

목차

소개

이 문서에서는 ESA(Email Security Appliance)에서 메일 루프를 식별하는 방법에 대해 설명합니다.

배경 정보

Mail Loops(메일 루프)는 3회 이상 삽입된 동일한 Message-ID의 메시지로 나타낼 수 있습니다.메일 루프는 CPU가 높고 전송 속도가 느리며 전반적인 성능 문제를 일으킬 수 있습니다.일반적으로 두 번 이상 삽입된 메시지 ID는 반복을 나타내지만, 문제가 발생하여 두 번 이상 삽입되거나 동일한 스팸 메시지를 동일한 Message-ID로 계속 주입하는 어설픈 스패머일 수 있습니다.

일반적으로 메일 루프는 메일 서버에서 메일 서버로 끊임없이 이동하는 동일한 메시지 또는 메시지 집합을 전송하는 이메일 인프라 문제로 인해 발생합니다. 이러한 메시지는 오랫동안 이러한 방식으로 접대를 받을 수 있지만, 네트워크 대역폭이나 ESA 처리 비용이 발생하는 것은 아닙니다.

솔루션

메일 루프를 확인하는 것은, 만약 이것이 문제가 될 것이라고 의심한다면, 당신은 그것을 눈여겨봐야 할 필요가 있지만, 보통 꽤 쉽다.
시스템의 CLI(Command-Line Interface)에 로그인하여 다음 명령 중 하나 또는 둘 다를 실행하여 가장 좋은 이점을 얻을 수 있습니다.

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

특히 Message-ID의 검색에서 정확히 동일한 ID의 반복 인스턴스가 표시되면 메일 루프가 있음을 알 수 있습니다. 그러나 동일한 메시지를 되찾고 있는 메일 서버 중 하나가 Message-ID 헤더를 변경하거나 제거하는 데 도움이 될 수 있으므로 이 방법이 충분하지 않을 수도 있습니다. 따라서 Message-ID(메시지 ID) 확인으로 확인할 수 있는 항목이 없으면 Subject(제목) 확인을 시도해 보십시오.

Message-ID로 루프 메시지를 찾도록 관리했다고 가정하면 메시지와 해당 상위 연결(ICID)에 대한

다른 정보도 찾을 수 있습니다. 동일한 로그 라인에 메시지 ID와 MID가 있으면 다음을 수행할 수 있습니다.

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

결과 출력이 제공된 경우 관련 ICID 및 DCID를 찾아 다음을 수행할 수 있습니다.

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

이제 완전한 연결(메시지 트랜잭션)을 가져야 하며, 메시지 트랜잭션이 어디에서 왔는지, 어디에서 전달되었는지 확인할 수 있습니다(이미 발생한 경우). 루핑 메시지를 확인한 후 다음 단계는 문제를 해결할 수 있도록 메시지를 확인하는 것입니다. 루프의 원인을 수정하지 않으면 이 메시지와 다른 메시지가 계속 반복되거나 문제가 곧 다시 발생할 가능성이 높습니다.

다음과 유사한 메시지 필터를 만듭니다.

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

이제 변경 사항을 커밋하고 다음 명령을 실행하여 메시지를 체크 아웃합니다.

```
tail looper
```

메일 로그 및 메시지 자체를 보고 얻을 수 있는 기타 정보를 통해 원격 시스템에 대한 정보를 얻을 수 있으므로 문제가 어디에 있는지 확인할 수 있어야 합니다.

메일 루프가 발생하지 않도록 하려면 어떻게 해야 합니까?

복잡한 환경에서는 이것이 어려울 수 있습니다. 즉, ESA나 다른 디바이스에서 새로운 네트워킹이 어떻게 변경되고 트래픽이 그 핵심 대상인지 파악하는 것입니다.실행 중인 메일 루프의 일반적인 원인 중 하나는 Received 헤더의 제거입니다. ESA는 메시지에서 100개의 Received 헤더가 표시될 때 메일 루프를 자동으로 탐지하고 중단하지만, ESA는 이 헤더의 제거를 허용하므로 메일 루프가 불량되는 경우가 많습니다. *정말* 정당한 이유가 없는 한, Received 헤더를 끄거나 제거하지 마십시오.

다음은 메일 루프를 방지하거나 수정하는 데 도움이 되는 필터 예입니다.

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
 if (header("X-ExtLoopCount2")) {
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
```

```
                $RemoteIP");}}
          else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
        else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
      else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
    else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
  else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```