ESA 스푸핑된 메일 필터링

목차

[소개](#)
[문제](#)
[솔루션](#)
[필터 적용](#)
[추가 조치](#)

소개

이 문서에서는 스팸 및 사기성 이메일이 네트워크에 유입될 때 Cisco ESA(Email Security Appliance)에서 발생하는 문제에 대해 설명합니다.

문제

사기 행위자가 전자 메일을 가장하려고 시도합니다.이메일이 회사 직원을 가장하는 경우(소속 직원을 대상으로 하는 경우), 특히 기만적일 수 있으며 혼란을 일으킬 수 있습니다.이 문제를 해결하기 위해 이메일 관리자는 회사 내에서 시작된 것으로 보이는 인바운드 메일(스푸핑된 메일)을 차단하려고 시도할 수 있습니다.

회사 반환 주소가 도메인 이름에 있는 인터넷에서 오는 인바운드 메일을 차단하면 문제가 해결되는 것 같습니다.죄송합니다. 이러한 방식으로 메일을 차단하면 합법적인 이메일도 동시에 차단할 수 있습니다.다음 예를 고려하십시오.

- 직원이 ISP 메일 서버로 모든 SMTP(Simple Mail Transfer Protocol) 트래픽을 투명하게 리디렉션하는 호텔 ISP(Internet Service Provider)를 이동하고 사용합니다.메일을 보낼 때 엔터프라이즈 SMTP 서버를 통해 직접 이동하는 것처럼 보일 수 있지만 실제로 엔터프라이즈에 전달되기 전에 서드파티 SMTP 서버를 통해 전송됩니다.

- 직원이 이메일 토론 목록에 가입합니다.메시지가 이메일 목록으로 전송되면 발신자에서 온 것으로 보이는 모든 가입자에게 반환됩니다.

- 외부 시스템은 외부에서 볼 수 있는 장치의 성능 또는 연결성을 모니터링하기 위해 사용됩니다.경고가 발생하면 이메일에 반환 주소에 회사 도메인 이름이 포함됩니다.WebEx와 같은 서드파티 서비스 제공자는 이를 매우 자주 수행합니다.

- 임시 네트워크 컨피그레이션 오류로 인해 회사 내부에서 보내는 메일은 아웃바운드 리스너가 아니라 인바운드 리스너를 통해 전송됩니다.

- 회사 외부에 있는 사람이 원래 헤더가 아닌 새 헤더 라인을 사용하는 MUSA(Mail User Agent)를 사용하여 회사로 다시 전달한다는 메시지를 받습니다.

- Federal Express **배송 페이지** 또는 Yahoo **이메일** 페이지와 같은 인터넷 기반 애플리케이션은 회사를 다시 가리키는 반환 주소가 있는 합법적인 메일을 생성합니다. 이 메일은 합법적이며

회사 내부에서 보낸 소스 주소가 있지만 내부에서 만들어진 것은 아닙니다.
다음 예에서는 도메인 정보를 기반으로 인바운드 메일을 차단하면 오탐이 발생할 수 있음을 보여 줍니다.

솔루션

이 섹션에서는 이 문제를 해결하기 위해 수행해야 하는 권장 작업에 대해 설명합니다.

필터 적용

합법적인 이메일 메시지의 손실을 방지하려면 도메인 정보를 기반으로 인바운드 메일을 차단하지 마십시오.대신 이러한 유형의 메시지가 네트워크에 들어올 때 제목 줄에 태그를 지정할 수 있습니다. 이는 메시지가 위조될 수 있음을 수신자에게 나타냅니다. 메시지 필터나 콘텐츠 필터를 사용하여 이 작업을 수행할 수 있습니다.

이러한 필터의 기본 전략은 뒤로 가리킬 본문 헤더 줄(**From** 데이터가 가장 중요)과 RFC 821 봉투 발신자를 확인하는 것입니다.이러한 헤더 라인은 MUA에서 가장 일반적으로 표시되며, 부정 행위자에 의해 위조될 가능성이 가장 높습니다.

다음 예제의 메시지 필터는 잠재적으로 가장된 메시지에 태그를 지정하는 방법을 보여줍니다.이 필터는 다음과 같은 여러 작업을 수행합니다.

- 제목 줄에 이미 **"{Positive Forged}"이(가)** 있는 경우 필터에 의해 다른 복사본이 추가되지 않습니다.메시지 흐름에 회신이 포함되어 있을 때 메시지 스레드가 완료되기 전에 제목이 메일 게이트웨이를 여러 번 통과할 수 있습니다.

- 이 필터는 도메인 이름 **@yourdomain.com**에 끝나는 주소가 **있는** Envelope Sender 또는 From 헤더를 **검색합니다**.mail-from 검색은 대소문자를 구분하지 않지만 from-header 검색은 대소문자를 구분하지 않습니다.두 위치 모두에서 도메인 이름이 발견되면 필터는 제목 줄 **끝에 "{Possible Forged}"**을 삽입합니다.

다음은 필터의 예입니다.

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com")
       {
           strip-header("Subject");
           insert-header("Subject", "$Subject {Possibly Forged}");
       }
   }
```

추가 조치

합법적인 메일에서 스푸핑된 메일을 식별하는 간단한 방법이 없기 때문에 문제를 완전히 제거할 방법이 없습니다.따라서 사기성 메일(피싱) 또는 스팸을 효과적으로 식별하고 이를 긍정적으로 차단하는 IPAS(IronPort Anti-Spam Scanning)를 활성화하는 것이 좋습니다.이 안티스팸 스캐너를 이전 섹션에서 설명한 필터와 함께 사용하면 합법적인 이메일의 손실 없이 최상의 결과를 얻을 수 있습

니다.

네트워크에 들어오는 사기성 이메일을 식별해야 하는 경우 DKIM(Domain Keys Identified Mail) 기술의 사용을 고려하십시오.더 많은 설정이 필요하지만 피싱 및 사기성 이메일에 대한 적절한 조치입니다.

> **참고:**메시지 필터에 대한 자세한 내용은 Cisco Email Security Appliance 지원 페이지의 **AsyncOS 사용 설명서**를 참조하십시오.