Cisco ESA(Email Security Appliance)를 통해 조직에 스팸 가져오기

목차

소개

이 문서에서는 스팸 이메일이 조직에 들어갈 수 있는 5가지 방법에 대해 설명합니다.

방법

1. 합법적인 메시지/마케팅 메일

사용자가 합법적인 메시지를 선택했거나 해당 이름이 다른 조직에 판매되었습니다.첫 번째 경우 사용자는 목록에서 가입을 취소하는 단계를 수행해야 합니다.후자의 경우, 안티스팸 정의를 전역적으로 업데이트할 수 있도록 spam@access.ironport.com으로 메시지를 다시 전송하여 ESA의 전체 스팸 캡처율을 개선합니다.수신 메일 정책에서 마케팅 메일을 활성화하면 이 메시지가 "스팸"보다 "마케팅"이라는 인식을 변경하는 데 도움이 될 수 있습니다.

2. 안티스팸이 올바르게 업데이트되지 않습니다.

안티스팸이 비활성화되었거나 기능 키가 만료되었습니다.안티스팸이 업데이트되고 있는지 확인하려면 **GUI > 보안 서비스 > IronPort 안티스팸으로** 이동하십시오. 이 패널 내에서 최근 6시간 내에 규칙 집합 또는 엔진에 대한 업데이트를 확인해야 합니다.또한 상단의 이 탭에서 안티스팸 서비스가 활성화되었는지 확인할 수 있습니다.기능 키 상태를 검토하려면 시스템 관리 탭 > 기능 키로 이동하여 안티스팸 키의 상태를 확인할 수 있습니다.

3. 메일 정책 또는 메시지 필터

고객 메일 정책에 따라 특정 발신자 또는 수신자에 대해 안티스팸 보안 엔진을 비활성화하면 스팸이 조직에 유입될 수 있습니다. 스팸 필터링을 건너뛰는 또 다른 방법은 메시지 필터(CLI:**filters** 명령).

4. 메일 플로우 정책

메시지는 메시지의 ICID를 사용하여 분류됩니다.이 경우 안티스팸 보안 기능이 해제되어 메일 정책을 재정의할 수 있습니다.메일 로그를 확인하여 이를 확인할 수 있습니다. 로그 내에서 먼저 ICID를

검토하여 메시지를 분류한 SenderGroup을 파악해야 합니다.연결된 메일 플로우 정책을 검토합니다.AllowList에 많은 항목이 있는 경우 AntiSpam 엔진에서 항목이 검사되었는지 확인하기 위해 들어오는 일부 메시지를 검토해야 할 수 있습니다.메시지의 헤더를 열고 헤더 X-IronPort-Spam을 찾습니다. 헤더가 있으면 메시지가 엔진을 통과했음을 의미합니다.

5. 메시지가 스팸임

메시지가 실제 스팸입니다.메시지 추적 기능을 사용하여 안티스팸 엔진에서 메시지를 검사했음을 확인했습니다(메시지 추적에서 "CASE" 검색). 케이스 판정이 음수이고 메시지가 스팸으로 간주될 경우 원본 메시지를 spam@access.ironport.com으로 제출합니다.이는 최근 출시되고 있는 새로운 스팸 위협이나 재설계된 오래된 위협일 수 있습니다.

스팸 제출 처리는 자동 및 수동 프로세스이며 특정 제출 시 피드백이 없습니다.언제든지 Cisco TAC에 문의하고 평가 및 응답을 요청할 수 있습니다.