Cisco Email Security Appliance를 통해 시뮬레이션된 피싱 플랫폼 캠페인을 허용하는 방법

목차

소개

이 문서에서는 시뮬레이션된 피싱 플랫폼 캠페인을 성공적으로 허용하기 위한 Cisco ESA(Email Security Appliance)의 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ESA에서 메시지 및 콘텐츠 필터 생성
- HAT(Host Access Table)의 컨피그레이션입니다.
- Cisco ESA의 수신 이메일 파이프라인 이해

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

관리자는 피싱 플랫폼을 시뮬레이션하여 사이클의 일부로 피싱 캠페인을 실행하여 이메일 시스템을 소셜 엔지니어링 공격의 벡터로 사용하는 가장 큰 위협 중 하나를 관리할 수 있습니다.

문제

ESA가 이러한 시뮬레이션에 대해 준비되지 않은 경우 스캐닝 엔진이 피싱 캠페인 메시지를 차단하

여 시뮬레이션의 실패 또는 실효성을 낮추는 것이 일반적입니다.

솔루션

> **주의:** 이 컨피그레이션 예에서는 ESA가 전송률 조절 없이 대규모 시뮬레이션된 피싱 캠페인을 통과하도록 TRUSTED 메일 플로우 정책을 선택합니다. 대량의 지속적인 피싱 캠페인을 실행하면 이메일 처리 성능에 영향을 미칠 수 있습니다.

피싱 캠페인 메시지가 ESA 컨피그레이션의 보안 구성 요소에 의해 중지되지 않도록 하려면 해당 메시지를 배치해야 합니다.

1. 새 발신자 그룹 생성: **GUI > Mail Policies(메일 정책) > HAT Overview(HAT 개요)**를 *신뢰할 수 있는* 메일 플로우 정책에 바인딩합니다(또는 **GUI > Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책)**에서 유사한 옵션을 사용하여 새 정책을 생성할 수 있음).
2. 시뮬레이션된 피싱 플랫폼의 전송 호스트 또는 IP를 이 Sender Group에 추가합니다. 시뮬레이션된 피싱 플랫폼에 많은 IP가 있는 경우 부분 호스트 이름을 대신 추가하거나 해당하는 경우 IP 범위를 추가할 수 있습니다.
3. BLOCKLIST Sender Group 위에 있는 Sender Group을 주문하여 SBRS가 아닌 정적으로 일치하는지 확인합니다.
4. **GUI > Mail Policies > Mail Flow Policies > TRUSTED**(또는 새로 생성된 메일 플로우 정책)에서 *TRUSTED* 메일 플로우 정책에 대한 모든 보안 기능을 비활성화합니다.

Security Features	
Spam Detection:	○ Use Default (On) ○ On ◉ Off
AMP Detection	○ Use Default (On) ○ On ◉ Off
Virus Protection:	○ Use Default (On) ○ On ◉ Off
Sender Domain Reputation Verification:	○ Use Default (On) ○ On ◉ Off
Virus Outbreak Filters:	○ Use Default (On) ○ On ◉ Off
Advanced Phishing Protection:	○ Use Default (On) ○ On ◉ Off
Graymail Detection:	○ Use Default (On) ○ On ◉ Off
Content Filters:	○ Use Default (On) ○ On ◉ Off
Message Filters:	○ Use Default (On) ○ On ◉ Off

5. **변경 사항을 제출하고 커밋합니다.**

이전 AsyncOS v.14

> **주의:** 이 컨피그레이션 예에서는 ESA가 전송률 조절 없이 대규모 시뮬레이션된 피싱 캠페인을 통과하도록 TRUSTED 메일 플로우 정책을 선택합니다. 대량의 지속적인 피싱 캠페인을 실행하면 이메일 처리 성능에 영향을 미칠 수 있습니다.

피싱 캠페인 메시지가 ESA 컨피그레이션의 보안 구성 요소에 의해 중지되지 않도록 하려면 해당 메시지를 배치해야 합니다.

1. 새 발신자 그룹 생성: **GUI > Mail Policies(메일 정책) > HAT Overview(HAT 개요)**를 클릭하여 *TRUSTED* 메일 플로우 정책에 바인딩합니다.
2. 시뮬레이션된 피싱 플랫폼의 전송 호스트 또는 IP를 이 Sender Group에 추가합니다. 시뮬레이션된 피싱 플랫폼에 많은 IP가 있는 경우 부분 호스트 이름을 대신 추가하거나 해당하는 경우 IP 범위를 추가할 수 있습니다.
3. BLOCKLIST Sender Group 위에 있는 Sender Group을 주문하여 SBRS가 아닌 정적으로 일치하는지 확인합니다.
4. **이러한 변경 사항을 제출하고 커밋합니다.**
5. CLI로 이동하여 새 메시지 필터, **CLI > 필터를 추가하고** 구문을 복사 및 수정하고 필터를 추가합니다.
6.
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. 목록에서 메시지 필터를 위로 정렬하여 건너뛴 필터 작업을 포함하는 위의 다른 메시지 필터에서 건너뛸 수 없도록 합니다.
8. Enter 키를 눌러 AsyncOS의 기본 명령 프롬프트로 돌아가 "commit" 명령을 실행하여 변경 사항을 커밋합니다. (Ctrl+C를 클릭하지 마십시오. 모든 변경 사항이 지워집니다.)
9. **GUI> Mail Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터)로** 이동합니다.
10. 사용자 지정 헤더 **"x-sp"** 및 *메시지* 필터*에* 구성된 *고유 값*을 찾도록 "Other Header" 조건*으로* 새 수신 콘텐츠 필터를 생성하고 Skip Remaining Content Filters(***Final Action)를 구성합니다***.
11. 시뮬레이션된 피싱 메시지에 대해 다른 필터가 조치를 취하지 않도록 콘텐츠 필터를 "1"로 주문합니다.
12. **GUI > Mail Policies > Incoming Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**로 이동하고 필요한 정책에 콘텐츠 필터를 할당합니다.
13. **변경 사항을 제출하고 커밋합니다.**
14. 시뮬레이션된 피싱 플랫폼 캠페인을 실행하고 mail_logs/Message Tracking을 모니터링하여 플로우 및 정책 규칙 일치를 확인합니다.