AMP 커넥터 해결 방법 - AMP for Endpoints에 앞서 Windows 프로세스 시작

목차

소개

이 문서에서는 SPP(System Process Protection) 이전에 Windows 프로세스가 시작될 때 AMP(Advanced Malware Protection) for Endpoints에서 문제를 해결하는 단계에 대해 설명합니다.

기고자: Nancy Perez와 Uriel Tores, Cisco TAC 엔지니어

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows OS
- AMP 커넥터의 엔진

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows 10 장치
- AMP 커넥터 6.2.9 버전

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.

제한 사항

이 버그는 AMP 커넥터 CSCvo90440 이전에 프로세스가 시작될 때 시스템 프로세스 보호 엔진에 [영향을 미칩니다.](#)

배경 정보

AMP for Endpoints System Process Protection 엔진은 다른 프로세스에 의한 메모리 주입 공격으로부터 중요한 Windows 시스템 프로세스를 보호합니다.

SPP를 활성화하려면 AMP 콘솔에서 **Management(관리) > Policies(정책) >** *수정할 정책에서 수정을 클릭합니다.* **> Modes and Engines(모드 및 엔진) > System Process Protection(시스템 프로세스 보호)**에서 다음 세 가지 옵션을 확인할 수 있습니다.

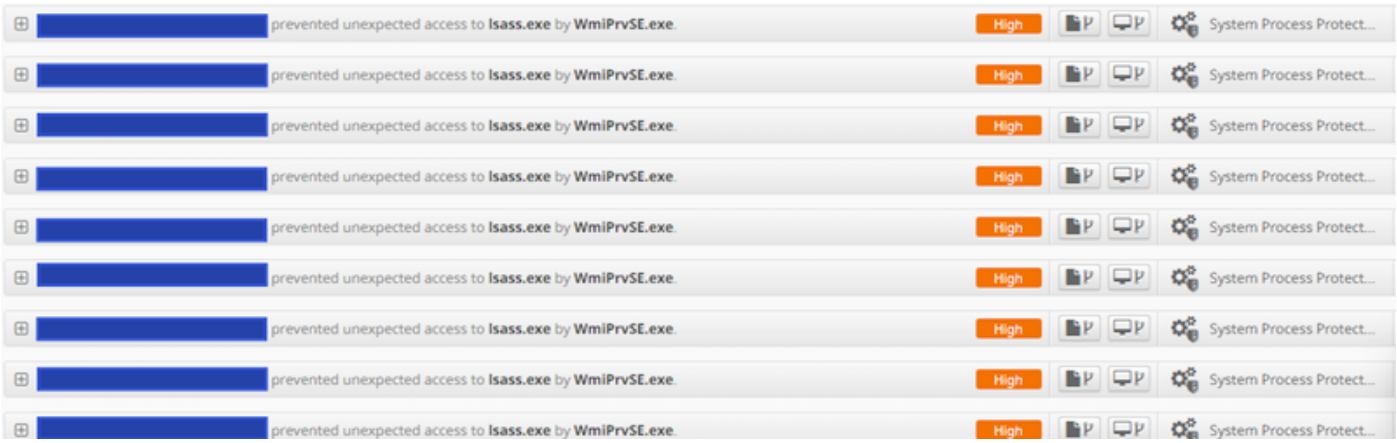
- 보호:중요한 Windows 시스템 프로세스에 대한 공격을 차단합니다.
- 감사:중요 Windows 시스템 프로세스에 대한 공격 알림
- 사용 안 함:이 모드에서는 엔진이 활성 상태가 아닙니다.

보호된 시스템 프로세스

시스템 프로세스 보호 엔진은 다음 프로세스를 보호합니다.

- 세션 관리자 하위 시스템(**smss.exe**)
- 클라이언트/서버 런타임 하위 시스템(**csrss.exe**)
- 로컬 보안 기관 하위 시스템(**lsass.exe**)
- Windows 로그온 응용 프로그램(**winlogon.exe**)
- Windows 시작 응용 프로그램(**wininit.exe**)

Windows 서비스가 AMP 커넥터(7.0.5 아래의 버전)보다 먼저 시작되면 시스템 프로세스 제외가 적용되지 않으며 프로세스가 제외되더라도 SPP 엔진이 프로세스를 중지하고 이미지에 표시된 대로 AMP 콘솔에 이벤트가 생성됩니다.



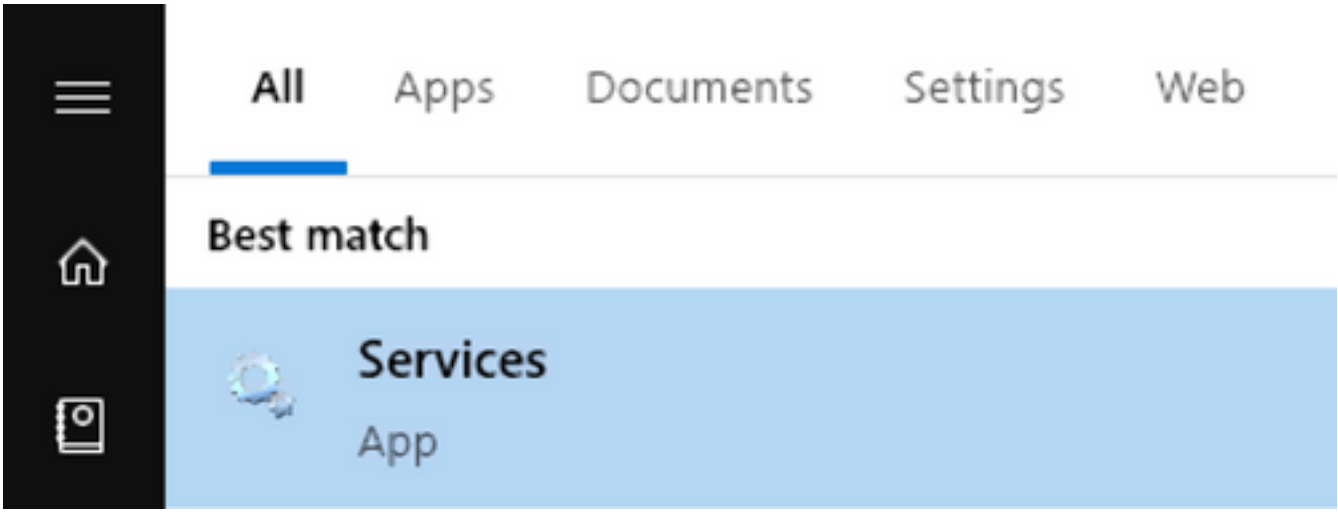
문제 해결

이 버그의 해결 방법은 AMP 서비스 전에 시작되는 Windows 서비스를 지연시키는 것입니다.

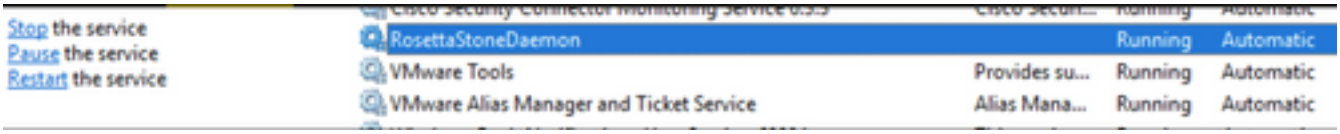
Rosetta Stone 응용 프로그램은 이 문서의 예제로 사용됩니다.이 응용 프로그램은 인증을 위해 lsass.exe 프로세스에 연결되므로 SPP에서 탐지됩니다.

Windows 서비스 지연 단계

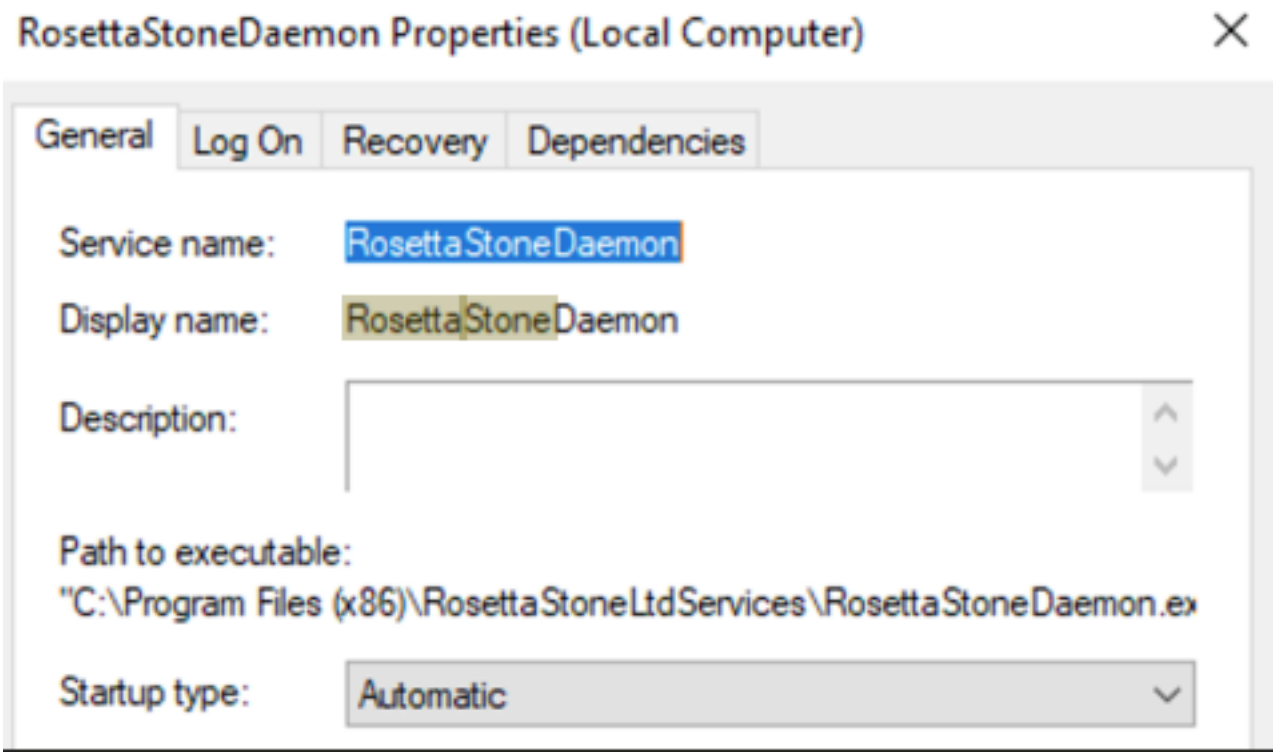
1단계. 이미지에 표시된 대로 services.msc를 엽니다.



2단계. Rosetta Stone 서비스를 찾습니다.

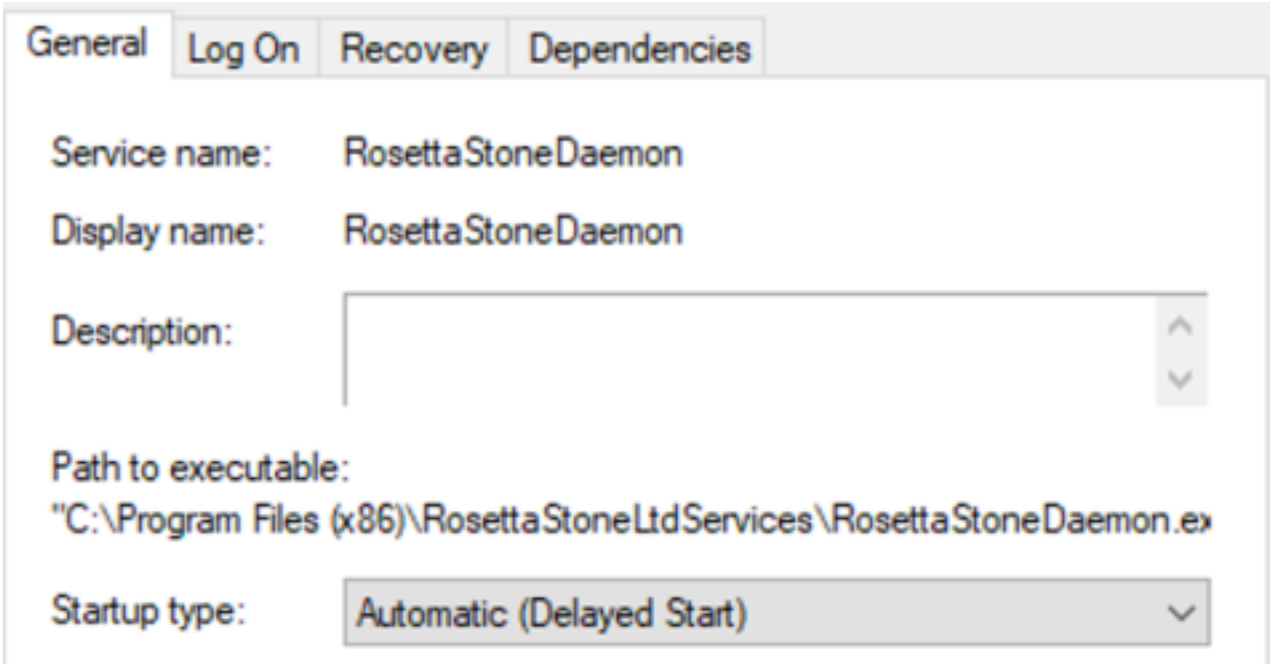


3단계. RosettaStoneDaemon을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다.



Startup 유형은 기본적으로 Automatic(자동)으로 구성되므로 RossettaStoneDaemon이 부팅 프로세스에서 자동으로 시작됩니다.

4단계. 드롭다운 메뉴를 클릭하고 자동(지연된 시작)을 선택합니다.



이 컨피그레이션은 AMP 커넥터 전에 RosettaStoneDaemon 서비스를 시작하지 못하게 합니다.

5단계. Apply(적용)를 클릭합니다.

명령줄을 사용하여 프로세스 지연

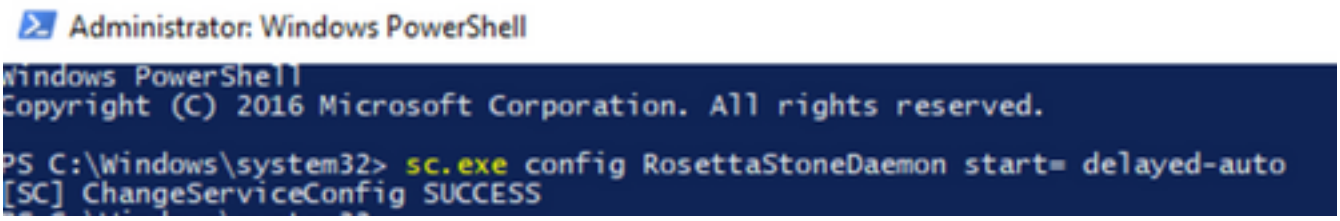
PowerShell/CMD의 경우 다음 명령을 사용할 수 있습니다.

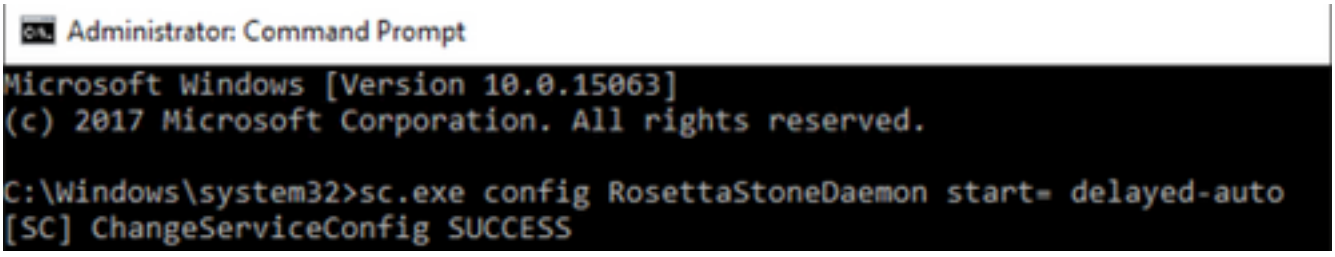
1단계. PowerShell/CMD를 관리자로 실행합니다.

2단계. 다음 명령을 실행합니다.

```
sc.exe config RosettaStoneDaemon start= delayed-auto
```

참고: Rosetta Stone = RosettaStoneDaemon.





이 섹션에서는 지연시킬 프로세스에 대해 RosettaStoneDaemon의 응용 프로그램 이름을 바꿀 수

있습니다.

주의: 커넥터 버전 7.0.5 이상에서는 이 버그에 대한 솔루션을 이미 구현했습니다.이 해결 방법은 7.0.5 이하의 커넥터 버전에 사용됩니다.