

Windows進程在AMP聯結器解決方法之前啟動 — 面向終端的AMP

目錄

[簡介](#)

[需求](#)

[採用元件](#)

[限制](#)

[背景資訊](#)

[疑難排解](#)

[延遲Windows服務的步驟](#)

[使用命令列延遲進程](#)

簡介

本文說明當系統進程保護(SPP)之前Windows進程啟動時，在面向終端的高級惡意軟體防護(AMP)中進行故障排除的步驟。

作者：Nancy Perez和Uriel Torres，思科TAC工程師。

需求

思科建議您瞭解以下主題：

- Windows作業系統
- AMP聯結器的引擎

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Windows 10裝置
- AMP聯結器6.2.9版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

限制

這是一個錯誤，當進程在AMP聯結器[CSCvo90440之前啟動時，它會影響系統進程保護引擎。](#)

背景資訊

面向終端的AMP系統進程保護引擎可保護關鍵Windows系統進程免受其他進程的記憶體注入攻擊。

若要啟用SPP，請在AMP控制檯上導航到**Management > Policies >** 在要修改的策略中點選**edit > Modes and Engine > System Process Protection**，您可以在此處找到三個選項：

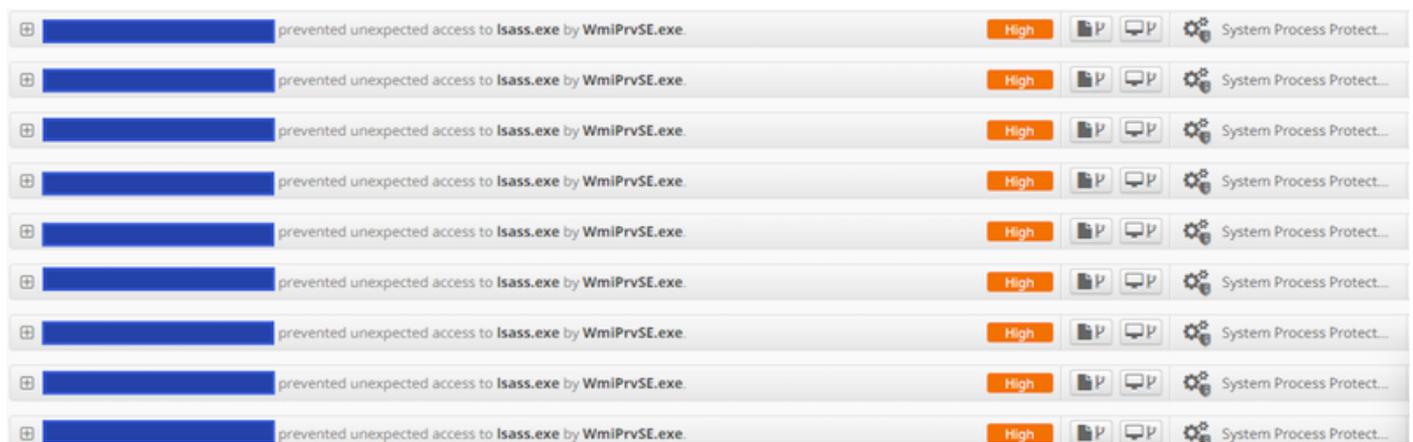
- 保護：阻止對關鍵Windows系統進程的攻擊
- 稽核：通知對關鍵Windows系統進程的攻擊
- 已禁用：引擎在此模式下未處於活動狀態

受保護系統進程

System Process Protection引擎可保護以下進程：

- 會話管理器子系統(**smss.exe**)
- 客戶端/伺服器運行時子系統(**csrss.exe**)
- 本地安全授權子系統(**lsass.exe**)
- Windows登入應用程式(**winlogon.exe**)
- Windows啟動應用程式(**wininit.exe**)

當Windows服務在AMP聯結器（7.0.5以下版本）之前啟動時，系統進程排除項不會執行，即使進程被排除，SPP引擎也會停止進程，並在AMP控制檯中建立一個事件，如下圖所示。



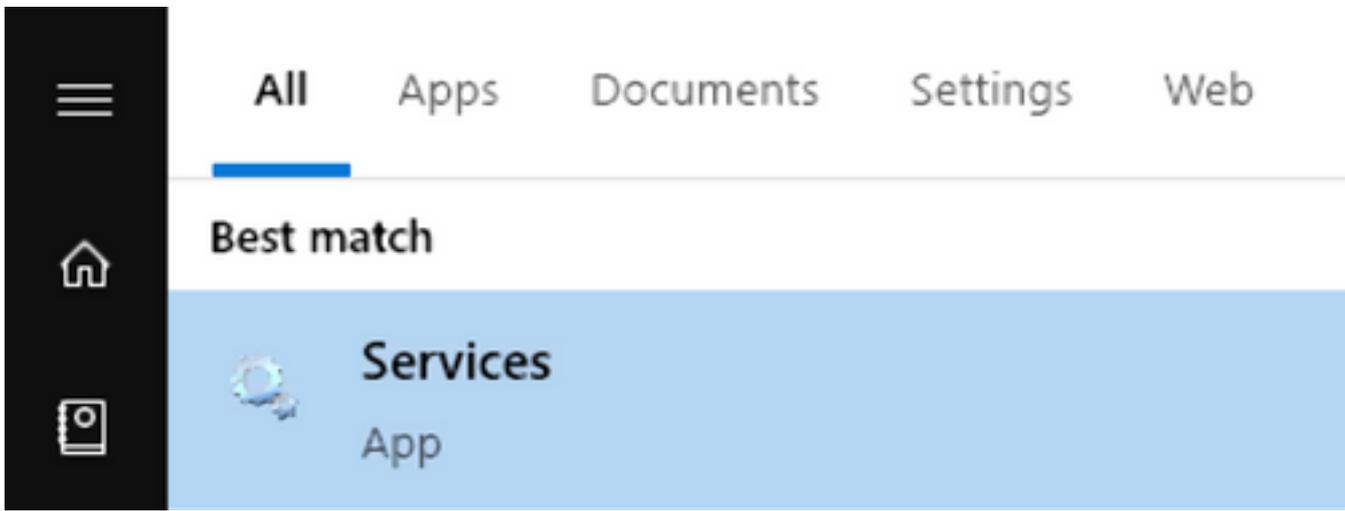
疑難排解

此錯誤的解決方法是延遲AMP服務之前啟動的Windows服務。

本文以Rosetta Stone應用程式為例。SPP檢測到此應用程式，因為它觸控lsass.exe進程以進行身份驗證。

延遲Windows服務的步驟

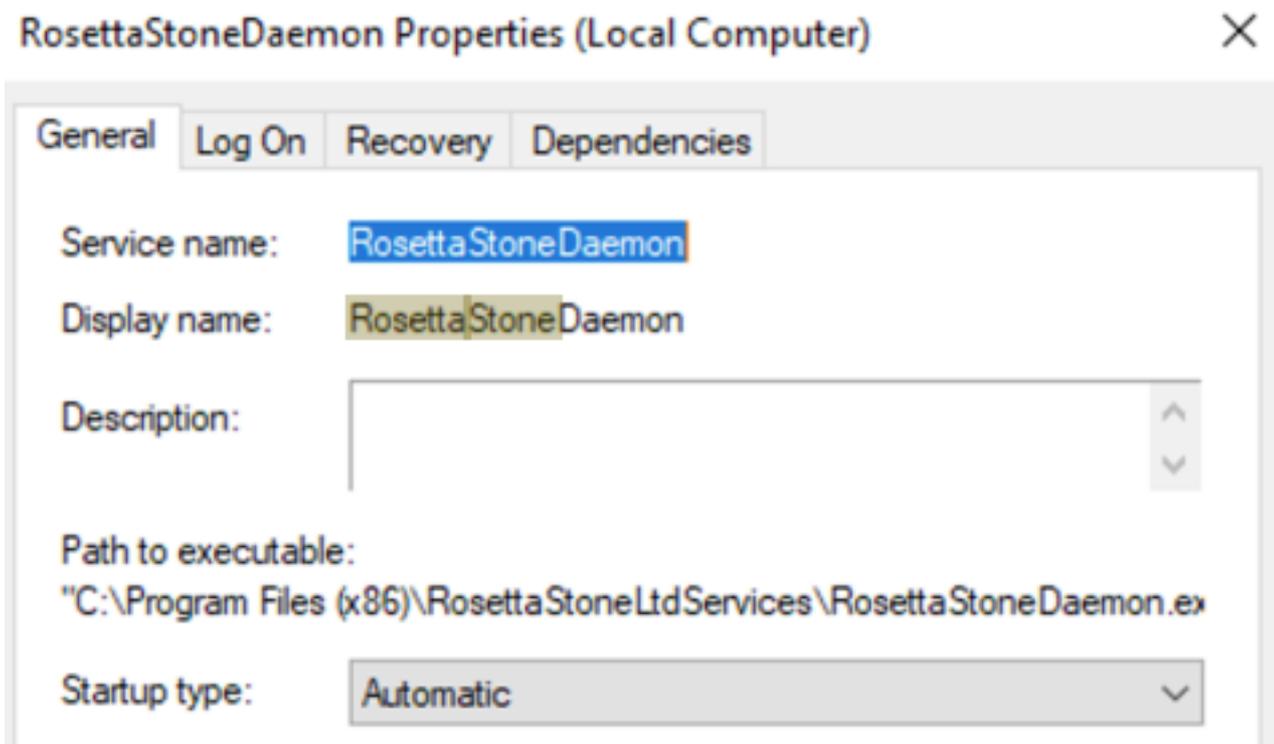
步驟1.開啟services.msc，如下圖所示。



步驟2.查詢Rosetta Stone服務。

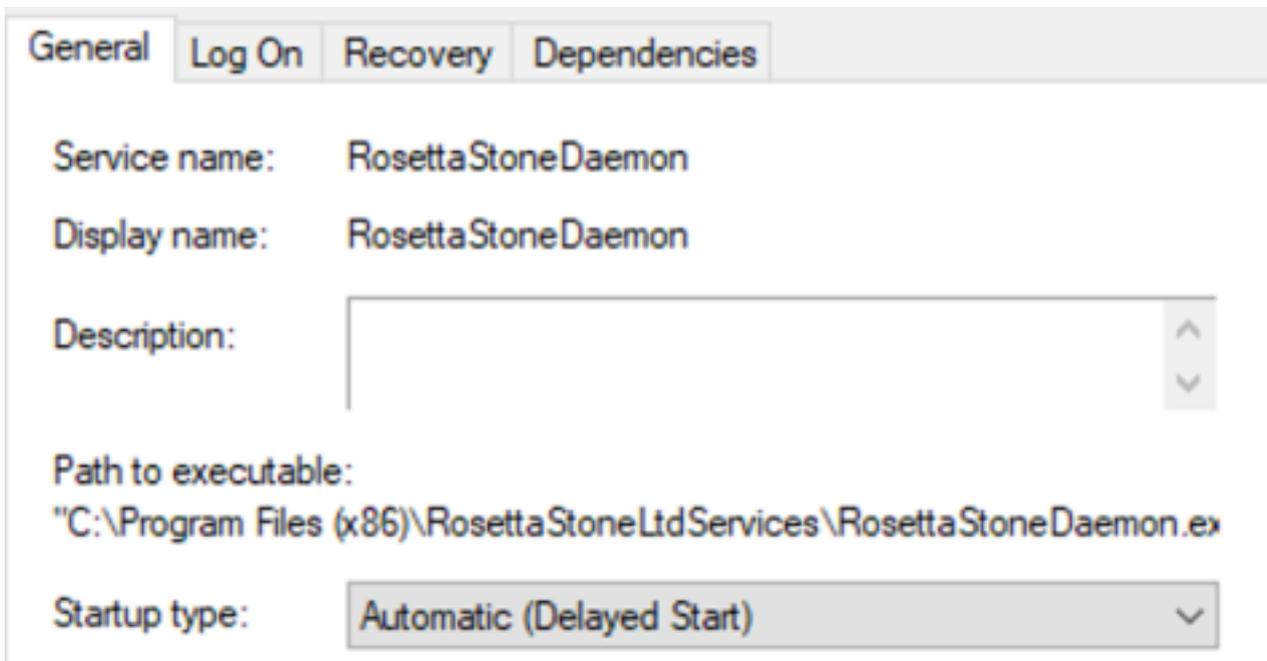
Service Name	Description	Status	Startup Type
Cisco Security Connector monitoring Service 0.0.0	Cisco Secur...	Running	Automatic
RosettaStoneDaemon		Running	Automatic
VMware Tools	Provides su...	Running	Automatic
VMware Alias Manager and Ticket Service	Alias Mana...	Running	Automatic

步驟3.按一下右鍵RosettaStoneDaemon，然後按一下「Properties (屬性)」。



預設情況下，「啟動」型別配置為「自動」，這意味著RosettaStoneDaemon在啟動過程中自動啟動。

步驟4.按一下下拉選單，然後選擇Automatic(Delayed Start)。



此配置可阻止RosettaStoneDaemon服務在AMP聯結器之前啟動。

步驟5.按一下Apply。



使用命令列延遲進程

對於PowerShell/CMD，可以使用以下命令。

步驟1.以管理員身份執行PowerShell/CMD。

步驟2.執行以下命令：

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

註:Rosetta Stone = RosettaStoneDaemon。

Administrator: Windows PowerShell

```
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Windows\system32> sc.exe config RosettaStoneDaemon start= delayed-auto  
[SC] ChangeServiceConfig SUCCESS
```

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.15063]  
(c) 2017 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>sc.exe config RosettaStoneDaemon start= delayed-auto  
[SC] ChangeServiceConfig SUCCESS
```

在本節中，可以為要延遲的進程替換RosettaStoneDaemon的應用程式名稱。

注意： 聯結器版本7.0.5及更高版本已實施針對此錯誤的解決方案。此解決方法適用於聯結器版本7.0.5以下。