Windows Process Starts Before AMP Connector Workaround - AMP for Endpoints

Contents

Introduction

This document describes the steps to troubleshoot in Advanced Malware Protection (AMP) for Endpoints when a Windows process starts before System Process Protection (SPP).

Contributed by Nancy Perez and Uriel Torres, Cisco TAC Engineers.

Requirements

Cisco recommends that you have knowledge of these topics:

- Windows OS
- AMP connector's engines

Components Used

The information in this document is based on these software and hardware versions:

- Windows 10 device
- AMP connector 6.2.9 version

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Limitations

This is a bug that affects the System Process Protection engine when a process starts before the AMP connector CSCvo90440.

Background Information

The AMP for Endpoints System Process Protection engine protects critical Windows system processes from memory injection attacks by other processes.

In order to enable SPP, on the AMP console, navigate to **Management > Policies >** *click on edit in the policy you want to modify* **> Modes and Engines > System Process Protection,** here you can find three options:

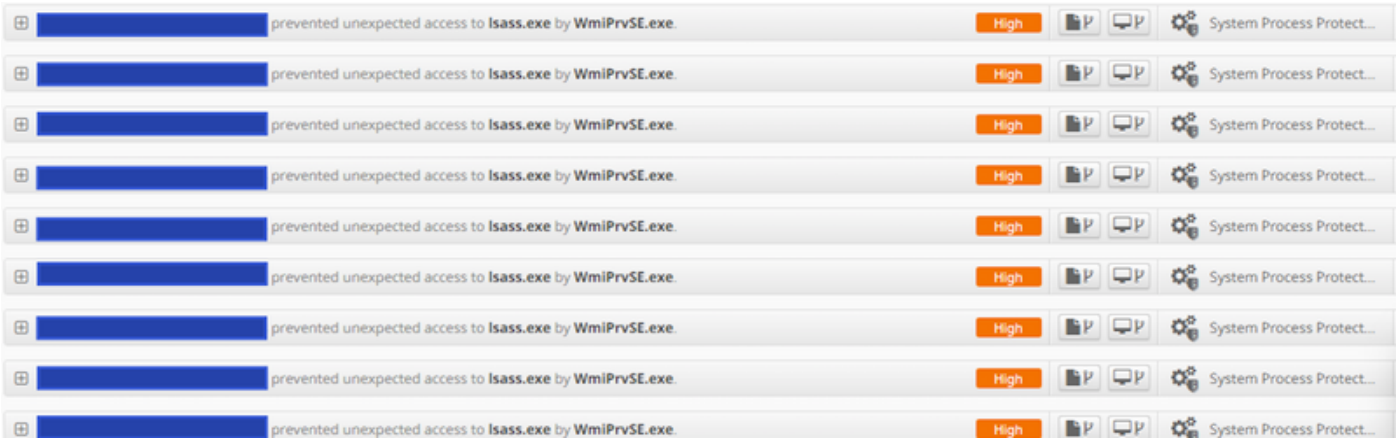
- Protect: blocks attacks on critical Windows system processes
- Audit: notify attacks on critical Windows system processes
- Disabled: the engine is not active on this mode

Protected System Processes

The System Process Protection engine protects the next processes:

- Session Manager Subsystem (**smss.exe**)
- Client/Server Runtime Subsystem (**csrss.exe**)
- Local Security Authority Subsystem (**lsass.exe**)
- Windows Logon Application (**winlogon.exe**)
- Windows Start-up Application (**wininit.exe**)

When a Windows Service starts before the AMP connector (In versions below the 7.0.5) System Process exclusions are not honored and even if a process is excluded, the SPP engine stops the process and an event is created in the AMP Console, as shown in the image.



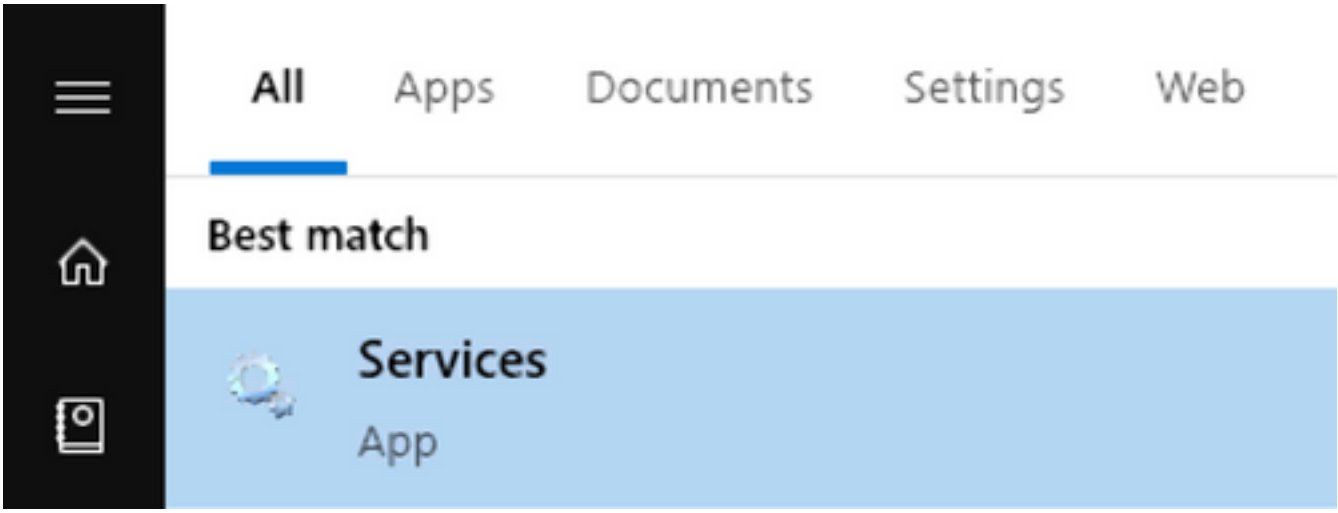
Troubleshoot

The workaround of this bug is to delay the Windows service that starts before the AMP service.

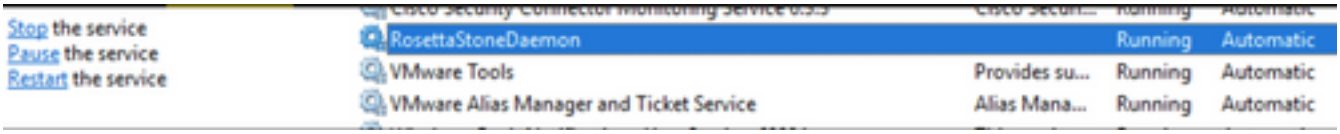
The Rosetta Stone application is taken as an example in this document. This application is detected by SPP because it touches the lsass.exe process for authentication purposes.

Steps to delay a Windows service

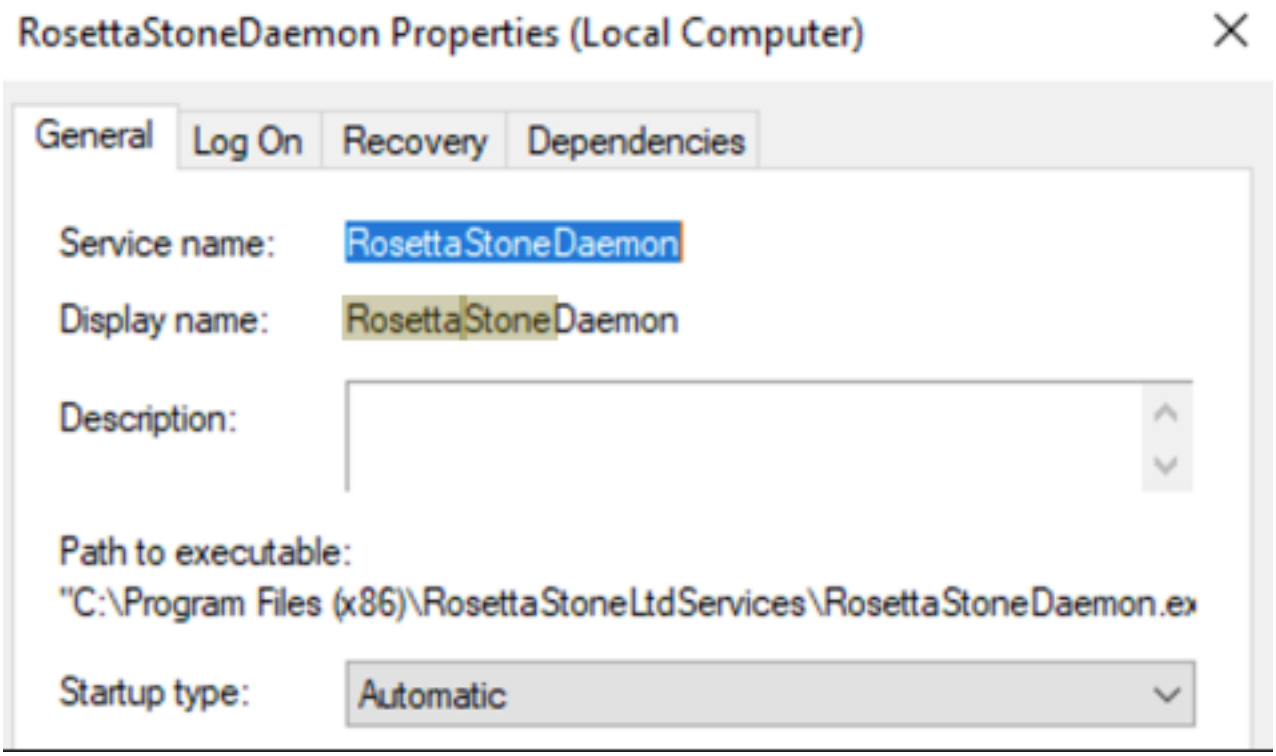
Step 1. Open services.msc, as shown in the image.



Step 2. Find Rosetta Stone service.

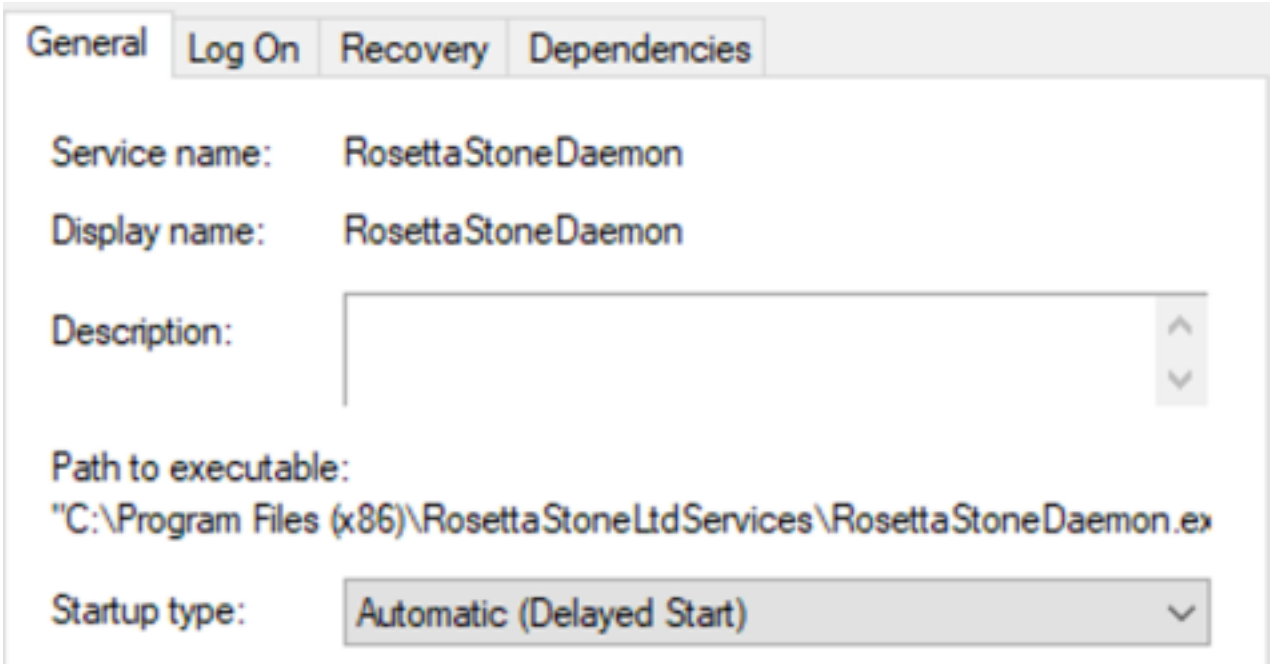


Step 3. Right-click on RosettaStoneDaemon and click on Properties.



The Startup type is configured as Automatic by default which means RossettaStoneDaemon starts automatically in the boot process.

Step 4. Click on the dropdown menu and select Automatic (Delayed Start).



This configuration prevents the RosettaStoneDaemon service starts before the AMP connector.

Step 5. Click on Apply.

Delay the process with the command line

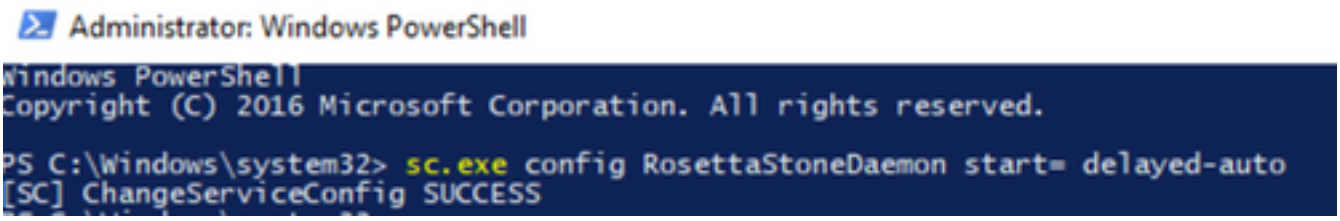
For PowerShell/CMD, the next commands can be used.

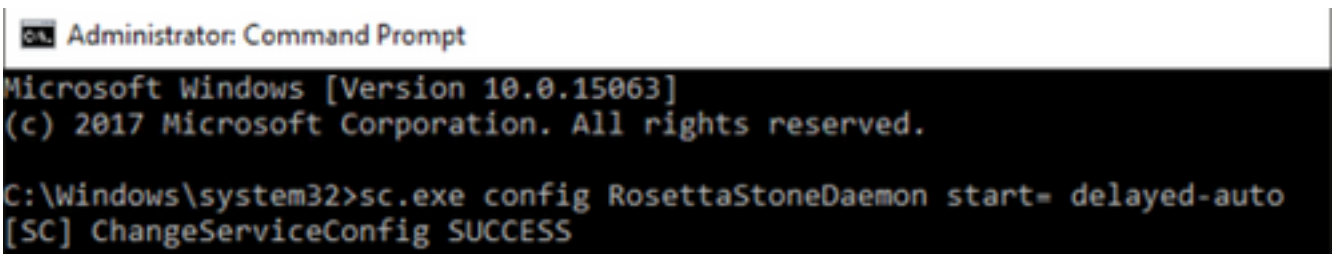
Step 1. Execute PowerShell/CMD as Administrator.

Step 2. Execute this command:

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

Note: Rosetta Stone = RosettaStoneDaemon.





In this section, you can replace the application name of RosettaStoneDaemon for the process you

want to delay.

> **Caution**: Connector version 7.0.5 and onward already implement a solution for this bug. This workaround is intended for connector versions bellow 7.0.5.