Windows-proces start voordat de AMP-connector aan de slag gaat - AMP voor endpoints

Inhoud

Inleiding

Dit document beschrijft de stappen naar probleemoplossing in Advanced Malware Protection (AMP) voor endpoints wanneer een Windows-proces start voordat System ProcProtection (SPP) wordt gestart.

Bijgedragen door Nancy Perez en Uriel Torres, Cisco TAC-engineers.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Windows OS
- Motoren van de AMP-connector

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows 10-apparaat
- AMP-aansluiting 6.2.9, versie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Beperkingen

Dit is een bug die de systeembeschermingsmotor beïnvloedt wanneer een proces start vóór de AMP-connector CSCvo90440.

Achtergrondinformatie

De Advanced Malware Protection-motor voor endpoints beschermt kritieke Windows-systeemprocessen tegen aanvallen door geheugeninjecties door andere processen.

Om SPP op de AMP-console in te schakelen, navigeer naar **Beheer > Beleid >** klik op *bewerk in het beleid dat u wilt wijzigen* **> Modi en motoren > Bescherming van systeemproces,** hier vindt u drie opties:

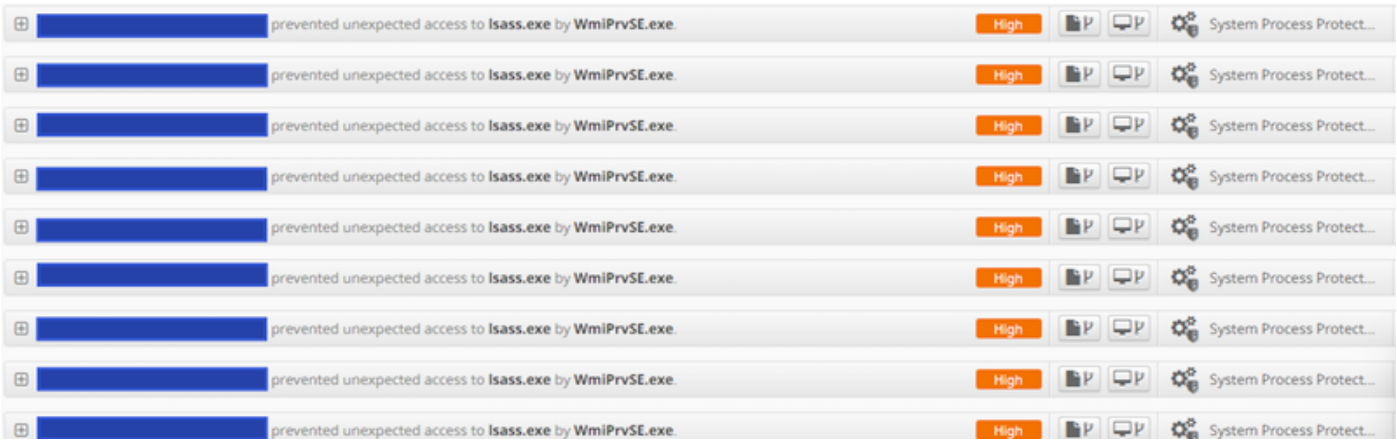
- Beschermen: blokkeert aanvallen op kritische Windows-systeemprocessen
- Audit: aanvallen op kritische Windows-systeemprocessen melden
- Uitgeschakeld: de motor is in deze stand niet actief

Beschermde systeemprocessen

De systeembeschermingsmotor beschermt de volgende processen:

- Session Manager-subsysteem (**smss.exe**)
- Subsysteem client/server (**csrss.exe**)
- Subsysteem Local Security Authority (**lsass.exe**)
- Windows Logon-toepassing (**winaanmelding.exe**)
- Windows Start-toepassing (**wininit.exe**)

Wanneer een Windows Service begint voordat de AMP-connector (In versies onder de 7.0.5) wordt de systeemuitsluitingen niet nageleefd en zelfs als een proces is uitgesloten, stopt de SPP-motor het proces en wordt er een gebeurtenis gecreëerd in de AMP-console, zoals in de afbeelding wordt getoond.



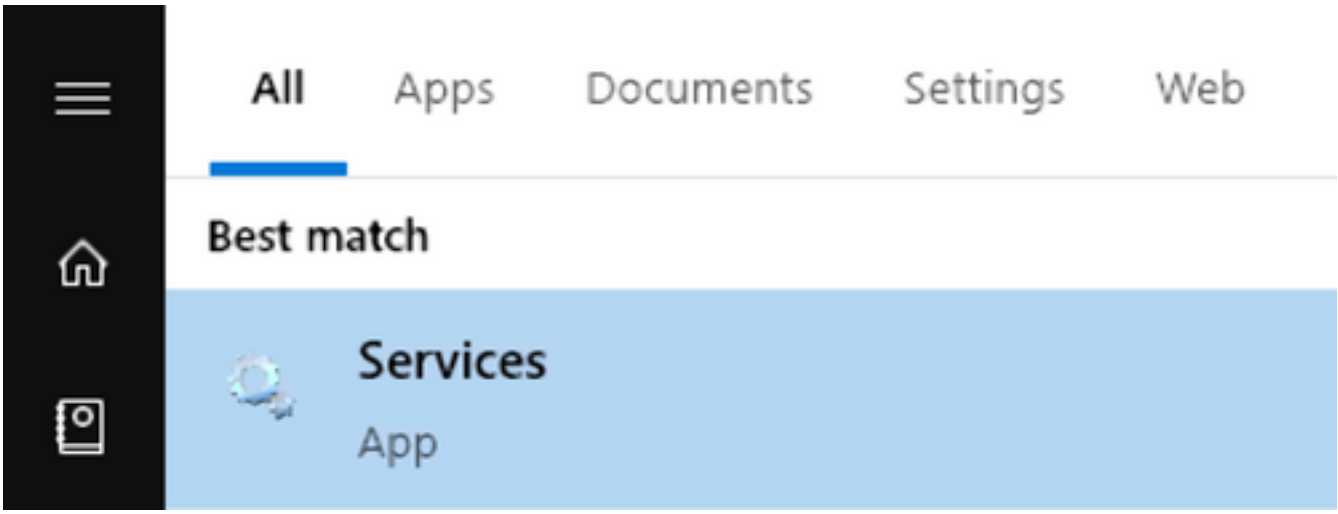
Problemen oplossen

De bewerking van dit bug is om de Windows-service uit te stellen die voor de AMP-service is gestart.

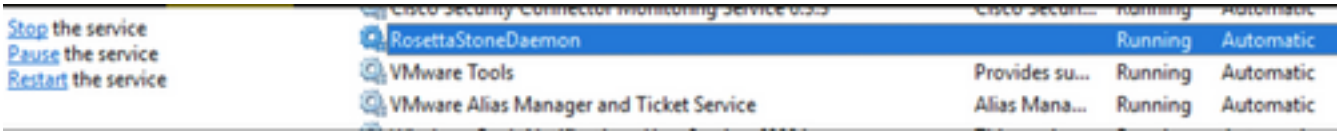
De toepassing van de Steen van Rosetta wordt in dit document als voorbeeld genomen. Deze toepassing wordt door SPP gedetecteerd omdat het het proces lsass.exe raakt voor authenticatiedoeleinden.

Stappen om een Windows-service uit te stellen

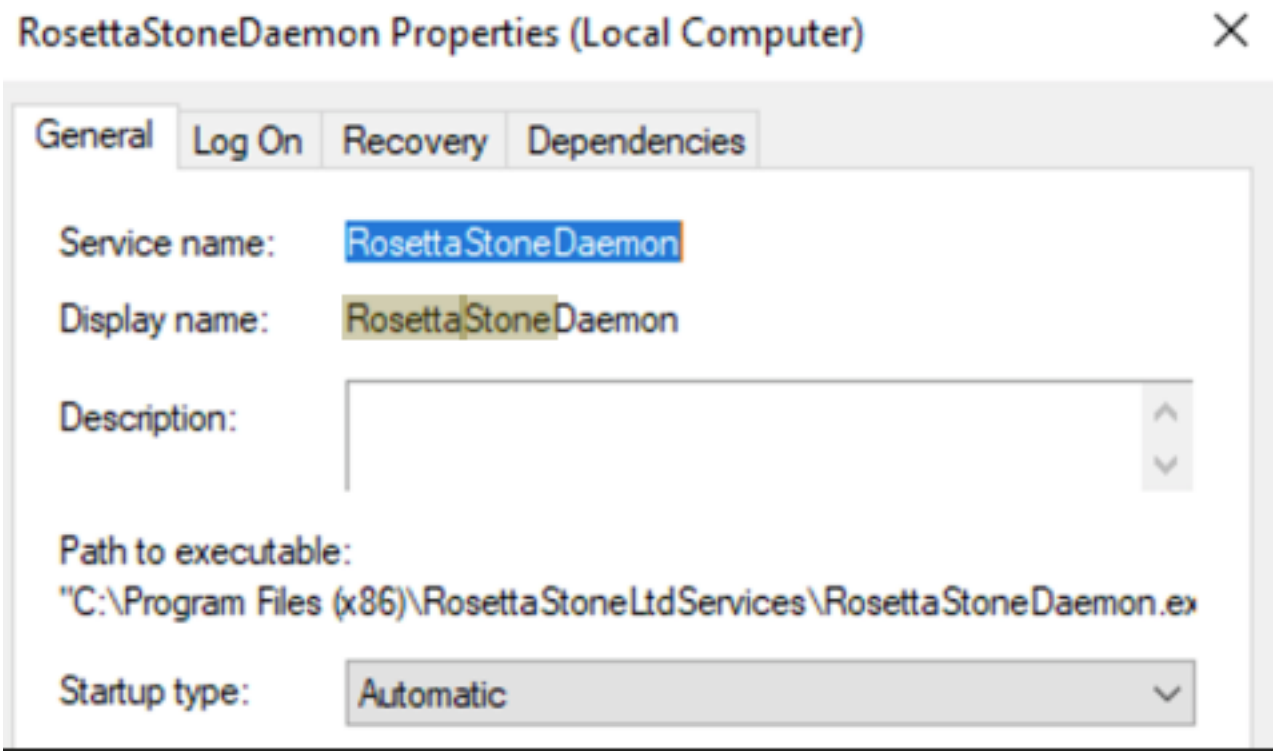
Stap 1. Open services.msc, zoals in de afbeelding.



Stap 2. Zoek de Stone-service van Rosetta.

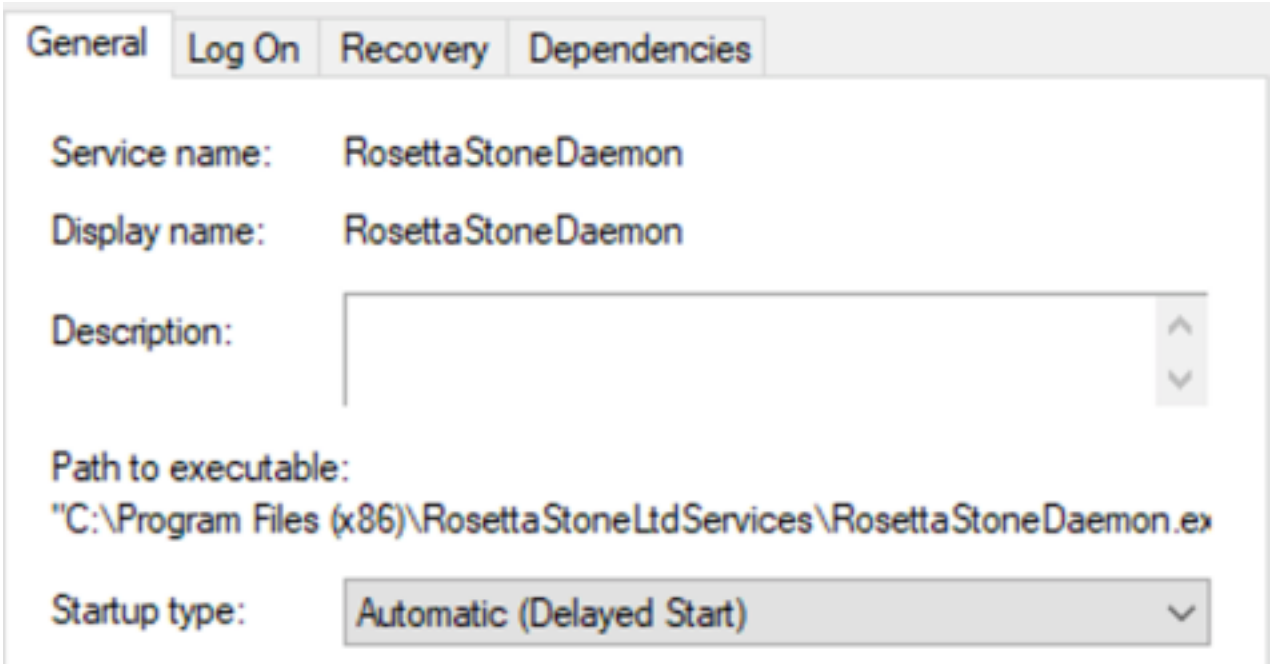


Stap 3. Klik met de rechtermuisknop op RosettaStoneDaemon en klik op Eigenschappen.



Het opstarttype is standaard ingesteld op Automatisch, dit betekent dat RossettaStoneDaemon automatisch start tijdens het opstarten.

Stap 4. Klik op het uitrolmenu en selecteer Automatisch (vertraagde start).



Deze configuratie voorkomt de RosettaStoneDaemon-service voordat de AMP-connector wordt gestart.

Stap 5. Klik op Toepassen.

Stel het proces uit met de opdrachtregel

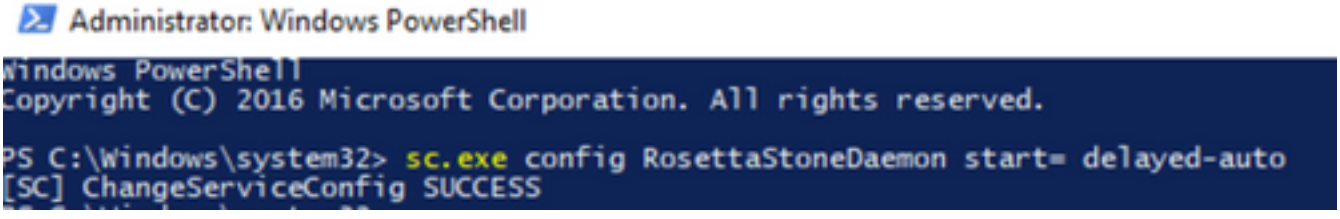
Voor PowerShell/CMD kunnen de volgende opdrachten worden gebruikt.

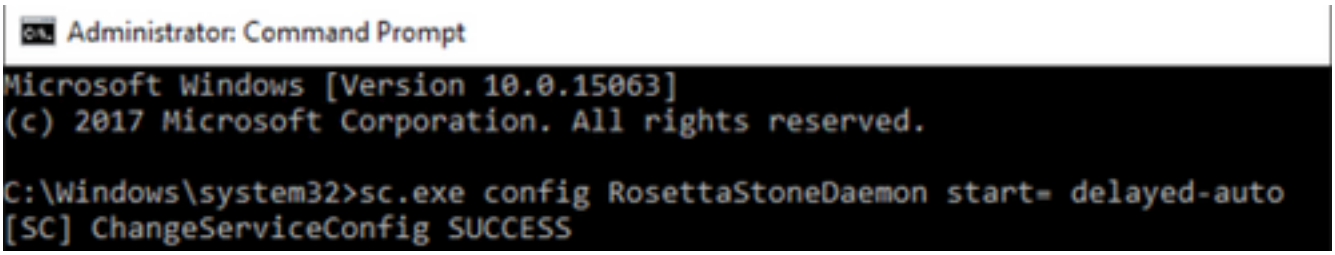
Stap 1. Voer PowerShell/CMD als beheerder uit.

Stap 2. Voer deze opdracht uit:

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

Opmerking: Rosetta Stone = RosettaStoneDaemon.





In deze sectie kunt u de toepassingsnaam van RosettaStoneDaemon vervangen voor het proces dat u wilt uitstellen.

> **Waarschuwing**: connector versie 7.0.5 en daarna voeren al een oplossing voor deze bug in. Deze tijdelijke versie is bedoeld voor aansluitversies onder 7.0.5.