El proceso de Windows comienza antes de la solución alternativa del conector de AMP: AMP para terminales

Contenido

Introducción

Este documento describe los pasos para solucionar problemas en la protección frente a malware avanzado (AMP) para terminales cuando se inicia un proceso de Windows antes de la protección de procesos del sistema (SPP).

Colaboración de Nancy Perez y Uriel Torres, Ingenieros del TAC de Cisco.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SO Windows
- Motores del conector AMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- dispositivo Windows 10
- conector AMP 6.2.9 versión

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Limitaciones

Se trata de un error que afecta al motor de protección del proceso del sistema cuando se inicia un proceso antes del conector de AMP [CSCvo90440.](#)

Antecedentes

El motor de protección de procesos del sistema de AMP para terminales protege los procesos críticos del sistema de Windows de ataques de inyección de memoria por parte de otros procesos.

Para habilitar SPP, en la consola de AMP, navegue hasta **Management > Policies >** *click on edit en la política que desea modificar* **> Modes and Engines > System Process Protection,** aquí encontrará tres opciones:

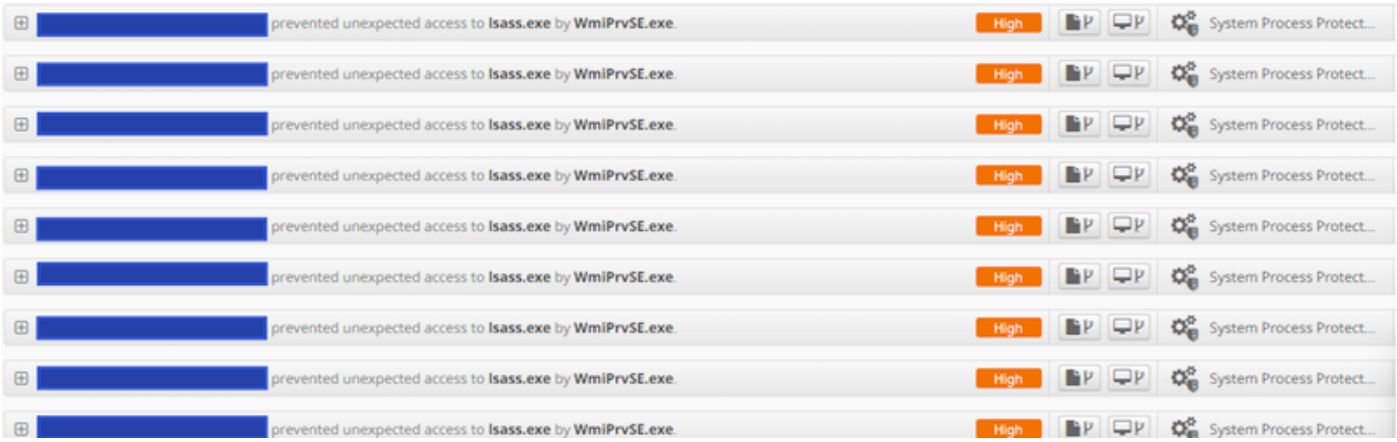
- Proteger: bloquea los ataques a los procesos críticos del sistema Windows
- Auditoría: notificar ataques a procesos críticos del sistema Windows
- Inhabilitado: el motor no está activo en este modo

Procesos del sistema protegidos

El motor System Process Protection protege los siguientes procesos:

- Subsistema del administrador de sesiones (**smss.exe**)
- Subsistema de tiempo de ejecución de cliente/servidor (**csrss.exe**)
- Subsistema de autoridad de seguridad local (**lsass.exe**)
- Aplicación de inicio de sesión de Windows (**winLogon.exe**)
- Aplicación de inicio de Windows (**wininit.exe**)

Cuando se inicia un servicio de Windows antes de que no se cumplan las exclusiones del proceso del sistema del conector de AMP (en las versiones siguientes a la 7.0.5) e incluso si se excluye un proceso, el motor SPP detiene el proceso y se crea un evento en la consola de AMP, como se muestra en la imagen.



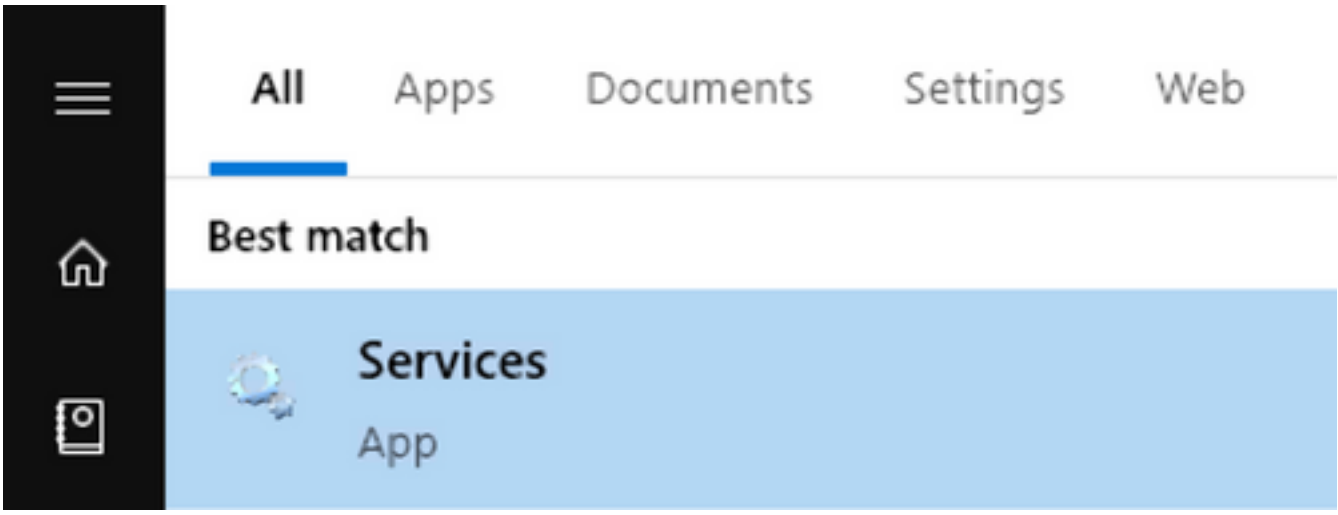
Troubleshoot

La solución temporal de este error es retrasar el servicio de Windows que se inicia antes del servicio AMP.

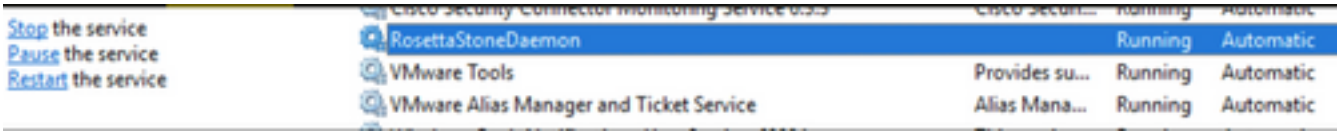
La aplicación Rosetta Stone se toma como ejemplo en este documento. SPP detecta esta aplicación porque toca el proceso lsass.exe con fines de autenticación.

Pasos para retrasar un servicio de Windows

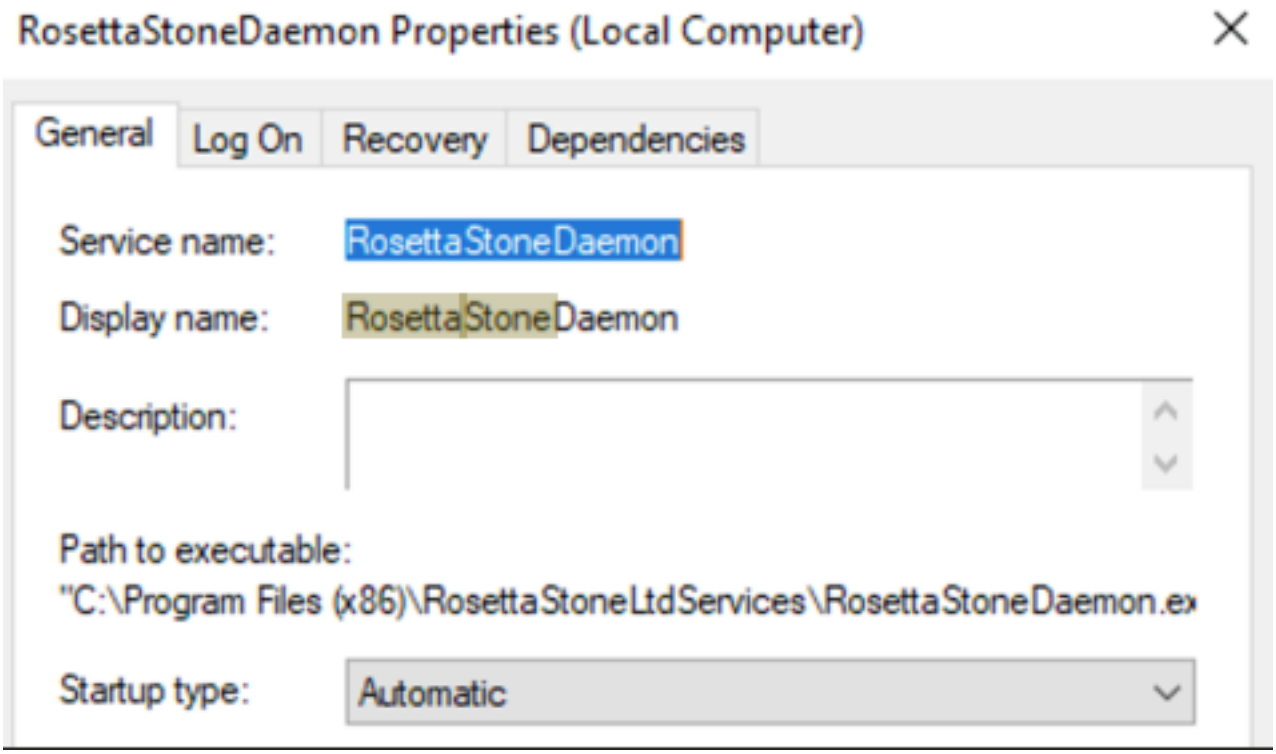
Paso 1. Abra services.msc, como se muestra en la imagen.



Paso 2. Encuentra el servicio Rosetta Stone.

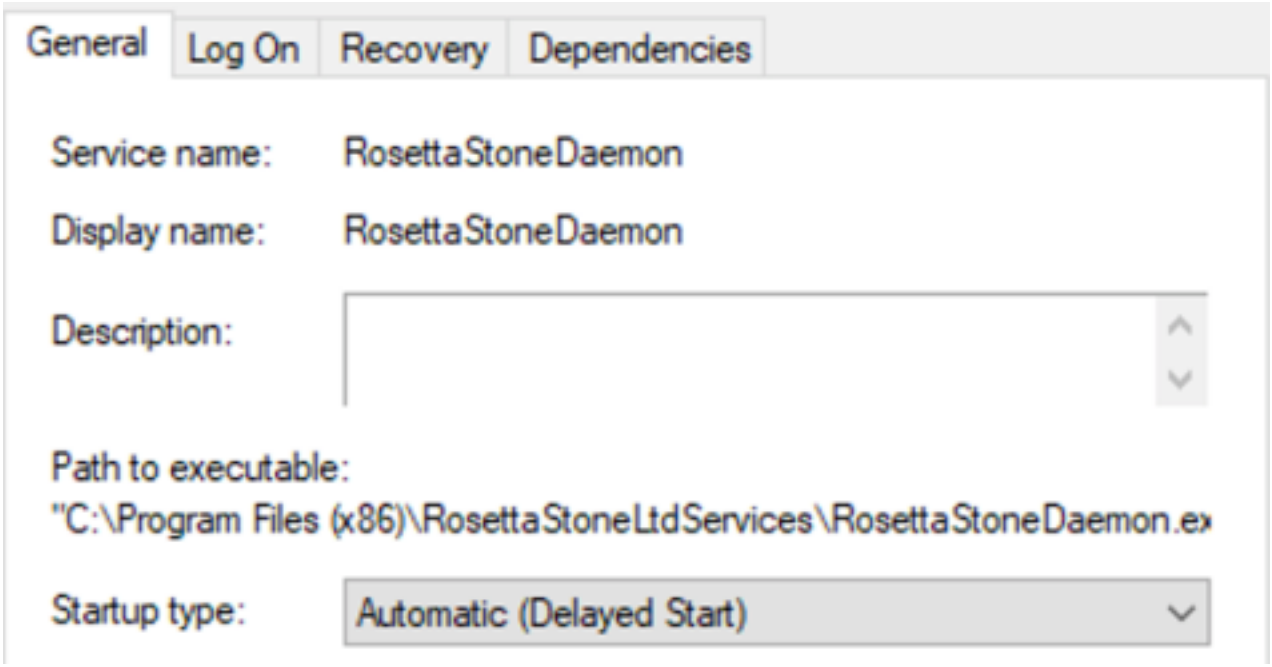


Paso 3. Haga clic con el botón derecho del ratón en RosettaStoneDaemon y haga clic en Propiedades.



El tipo de inicio se configura como Automático de forma predeterminada, lo que significa que RossettaStoneDaemon se inicia automáticamente en el proceso de inicio.

Paso 4. Haga clic en el menú desplegable y seleccione Automático (Inicio retrasado).



Esta configuración evita que se inicie el servicio RosettaStoneDaemon antes del conector de AMP.

Paso 5. Haga clic en Apply (Aplicar).

Retrasar el proceso con la línea de comandos

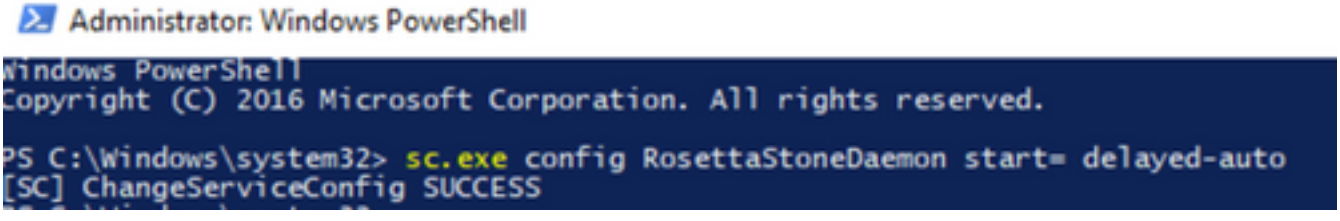
Para PowerShell/CMD, se pueden utilizar los siguientes comandos.

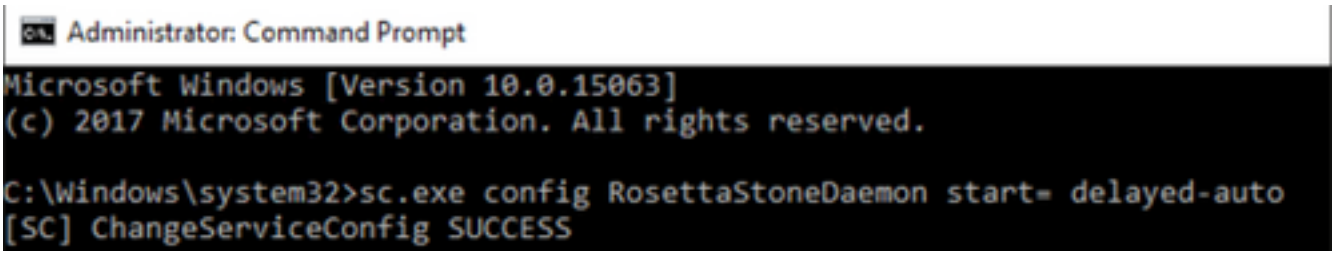
Paso 1. Ejecute PowerShell/CMD como administrador.

Paso 2. Ejecute este comando:

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

Nota: Rosetta Stone = RosettaStoneDaemon.





En esta sección, puede reemplazar el nombre de aplicación de RosettaStoneDaemon por el proceso que desea retrasar.

> **Precaución**: la versión 7.0.5 y posterior del conector ya implementan una solución para este bug. Esta solución alternativa está pensada para las versiones de conector siguientes a 7.0.5.