O processo do Windows começa antes da solução do conector AMP - AMP para endpoints

Contents

Introduction

Este documento descreve as etapas para solucionar problemas no AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints quando um processo do Windows é iniciado antes do SPP (System Process Protection, Proteção de processo do sistema).

Contribuído por Nancy Perez e Uriel Torres, engenheiros do TAC da Cisco.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SO Windows
- Mecanismos do conector AMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- dispositivo Windows 10
- Versão do conector AMP 6.2.9

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Limitações

Este é um bug que afeta o mecanismo System Process Protection quando um processo é iniciado antes do conector AMP [CSCvo90440.](#)

Informações de Apoio

O mecanismo AMP para Endpoints System Process Protection protege os processos críticos do sistema Windows de ataques de injeção de memória por outros processos.

Para habilitar o SPP, no console da AMP, navegue para **Management > Policies >** *click on edit na política que você deseja modificar* **> Modes and Engines > System Process Protection,** aqui você encontrará três opções:

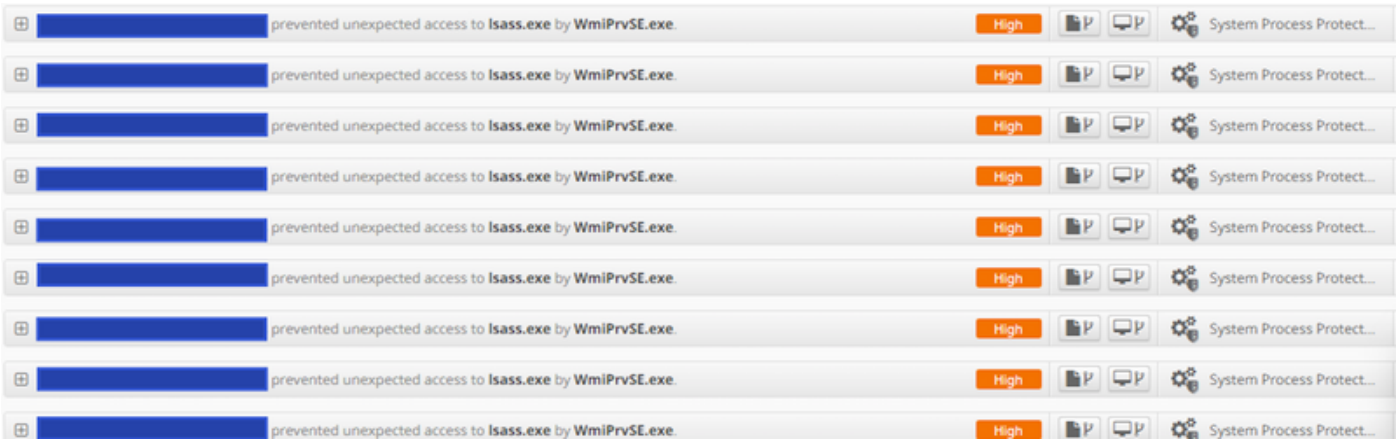
- Proteger: bloqueia ataques em processos críticos do sistema Windows
- Auditoria: notificar ataques em processos críticos do sistema Windows
- Desabilitado: o motor não está ativo neste modo

Processos de Sistema Protegido

O mecanismo de proteção de processos do sistema protege os próximos processos:

- Subsistema do Session Manager (**smss.exe**)
- Subsistema de Tempo de Execução do Cliente/Servidor (**csrss.exe**)
- Subsistema de Autoridade de Segurança Local (**lsass.exe**)
- Aplicativo de Início de Sessão do Windows (**winlogon.exe**)
- Aplicativo de Inicialização do Windows (**wininit.exe**)

Quando um Serviço do Windows é iniciado antes do conector AMP (em versões abaixo de 7.0.5), as exclusões do Processo do Sistema não são honradas e mesmo que um processo seja excluído, o mecanismo SPP interrompe o processo e um evento é criado no Console do AMP, como mostrado na imagem.



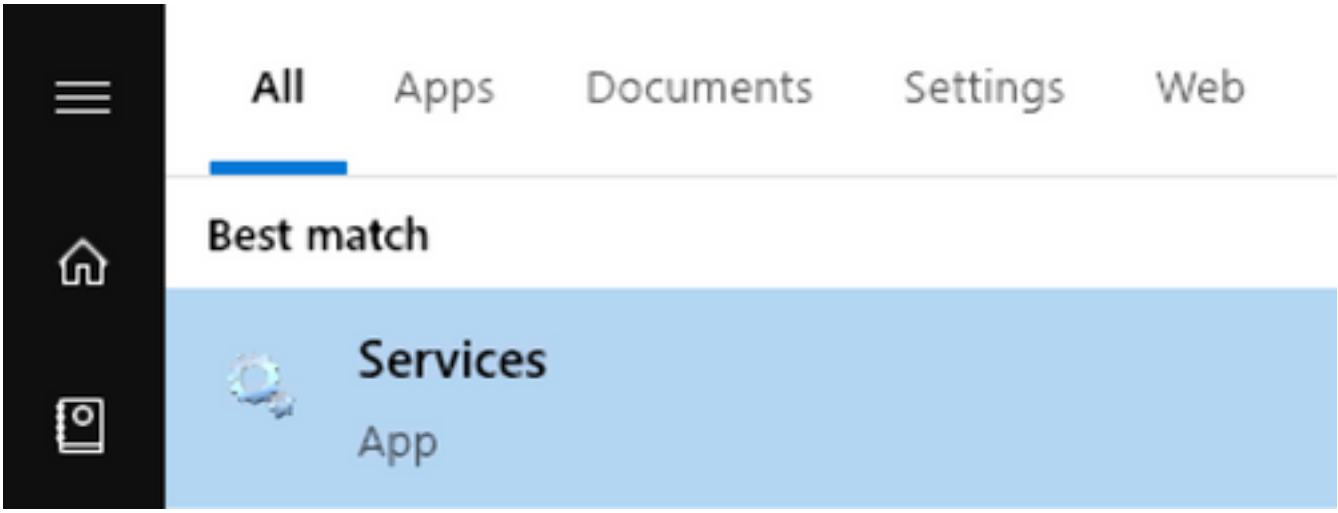
Troubleshoot

A solução alternativa deste bug é atrasar o serviço do Windows iniciado antes do serviço AMP.

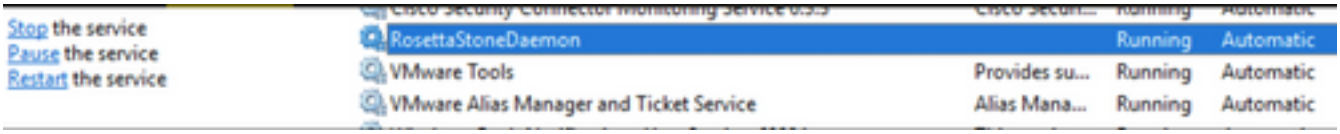
O aplicativo Rosetta Stone é tomado como exemplo neste documento. Este aplicativo é detectado pelo SPP porque toca no processo lsass.exe para fins de autenticação.

Etapas para atrasar um serviço do Windows

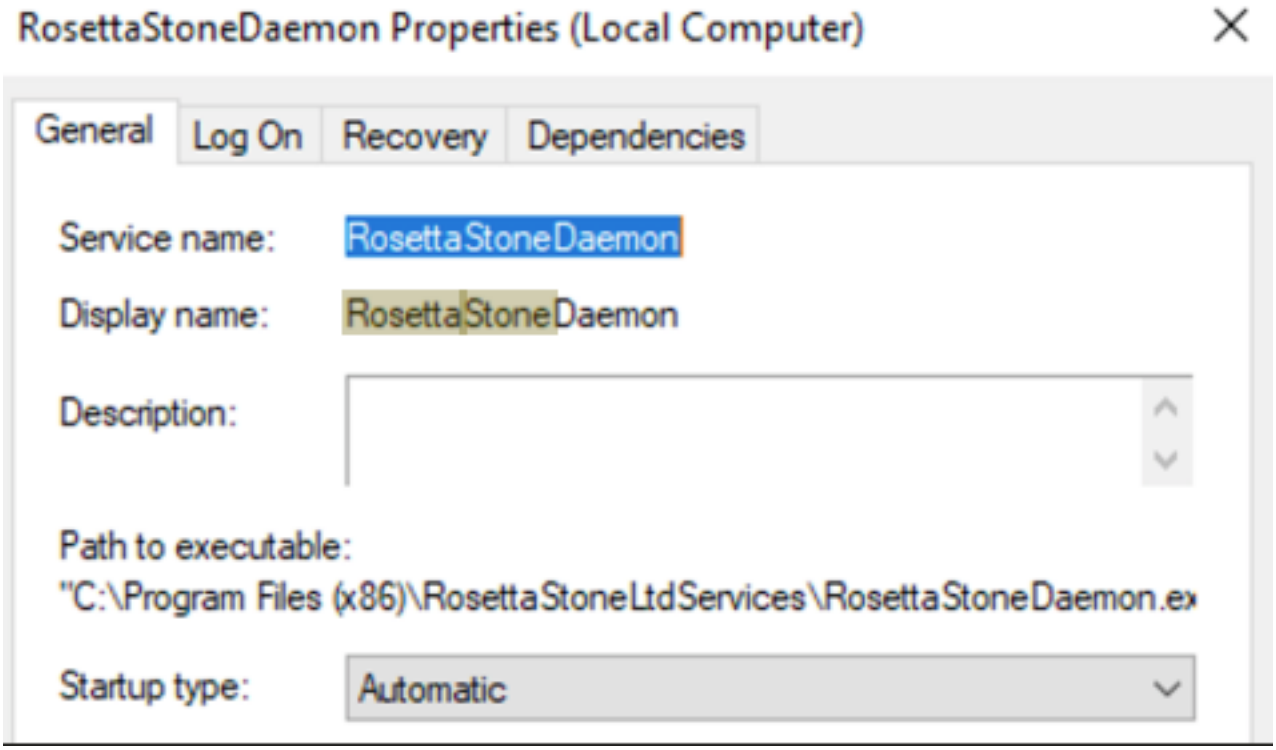
Etapa 1. Abra services.msc, como mostrado na imagem.



Etapa 2. Encontre o serviço Rosetta Stone.

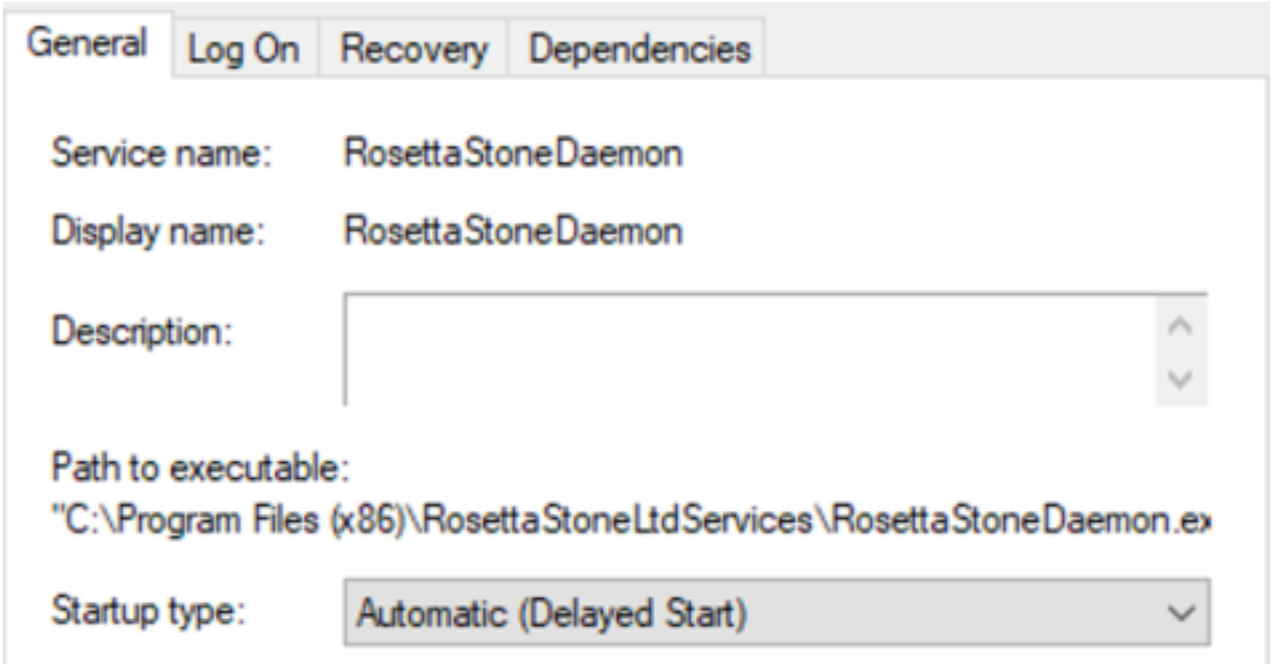


Etapa 3. Clique com o botão direito do mouse em RosettaStoneDaemon e clique em Propriedades.



O tipo de inicialização é configurado como Automático por padrão, o que significa que o RossettaStoneDaemon inicia automaticamente no processo de inicialização.

Etapa 4. Clique no menu suspenso e selecione Automático (Início atrasado).



Essa configuração impede que o serviço RosettaStoneDaemon seja iniciado antes do conector AMP.

Etapa 5. Clique em Apply (Aplicar).

Atrasar o processo com a linha de comando

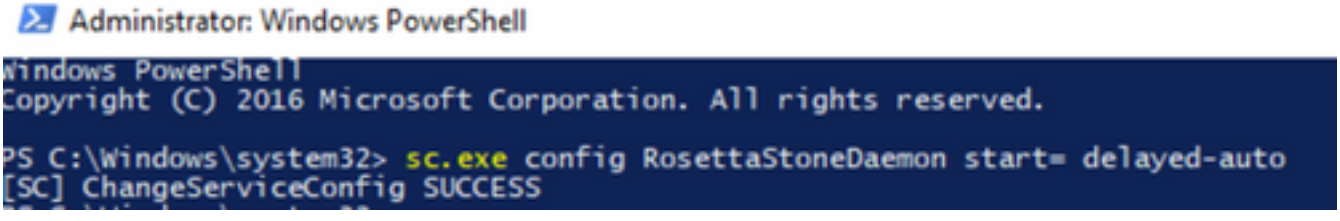
Para o PowerShell/CMD, os próximos comandos podem ser usados.

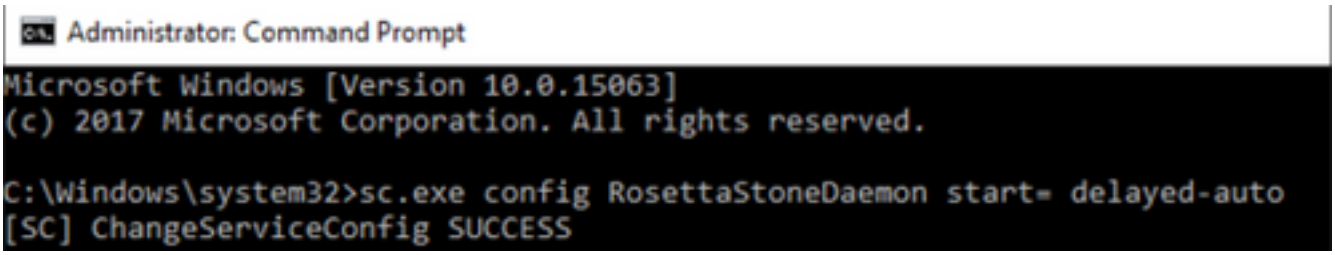
Etapa 1. Execute o PowerShell/CMD como administrador.

Etapa 2. Execute este comando:

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

Nota: Pedra de Rosetta = RosettaStoneDaemon.





Nesta seção, você pode substituir o nome do aplicativo RosettaStoneDaemon para o processo que deseja atrasar.

> Cuidado: o conector versão 7.0.5 e posteriores já implementam uma solução para esse bug. Esta solução alternativa destina-se a versões de conectores abaixo de 7.0.5.