Process starts de Windows avant contournement de connecteur d'AMP - AMP pour des points finaux

Contenu

Introduction

Ce document décrit les étapes pour dépanner dans la protection avancée de malware (AMP) pour des points finaux quand des process starts de Windows avant la protection de processus de système (espèces).

Contribué par Nancy Perez et Uriel Torres, ingénieurs TAC Cisco.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système d'exploitation windows
- Les engines du connecteur d'AMP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Périphérique de Windows 10
- Version du connecteur 6.2.9 d'AMP

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Limites

C'est une bogue qui affecte l'engine de protection de processus de système quand des process

starts avant le connecteur CSCvo90440 d'AMP.

Informations générales

L'AMP pour l'engine de protection de processus de système de points finaux protège des processus de système Windows essentiel contre des attaques d'injection de mémoire par d'autres processus.

Afin d'activer des espèces, sur la console d'AMP, naviguez vers la **Gestion > les stratégies >** *cliquent sur éditent en fonction dans la stratégie que vous voulez modifier* **> des modes et des engines > protection de processus de système,** ici vous pouvez trouver trois options :

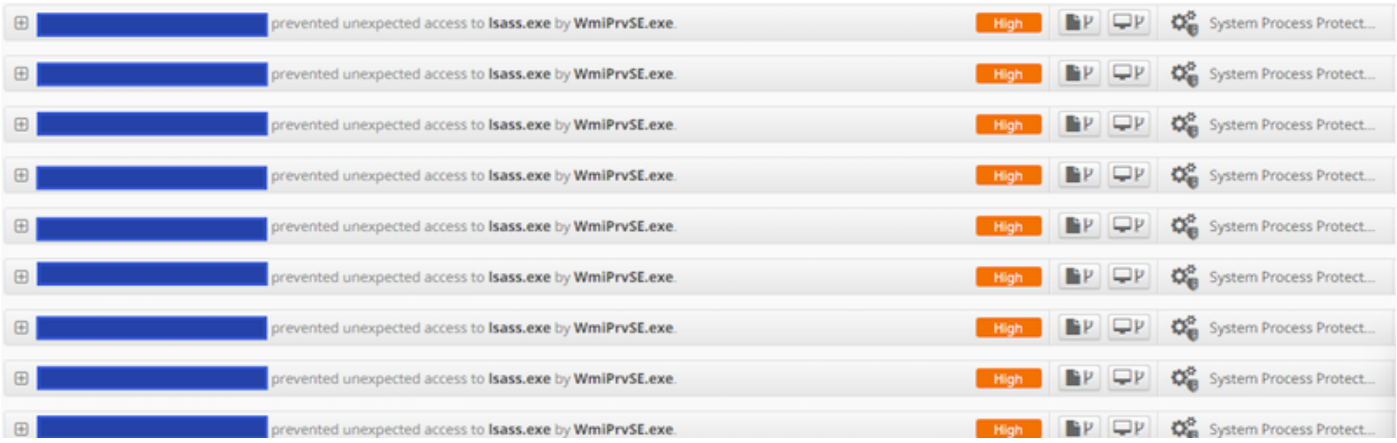
- Protégez : attaques de blocs sur des processus de système Windows essentiel
- Audit : informez les attaques sur des processus de système Windows essentiel
- Handicapé : l'engine n'est pas en activité sur ce mode

Processus protégés de système

L'engine de protection de processus de système protège les prochains processus :

- Sous-système de gestionnaire de session (**smss.exe)**
- Sous-système d'exécution de client/serveur (**csrss.exe)**
- Sous-système d'autorité de sécurité locale (**lsass.exe)**
- Application de connexion de Windows (**winlogon.exe)**
- Application de démarrage de Windows (**wininit.exe)**

Quand les débuts d'un service windows avant que les exclusions de processus de système de connecteur d'AMP (dans les versions au-dessous des 7.0.5) ne soient pas honorées et même si un processus est exclu, l'engine espèces arrête le processus et un événement est créé dans la console d'AMP, suivant les indications de l'image.



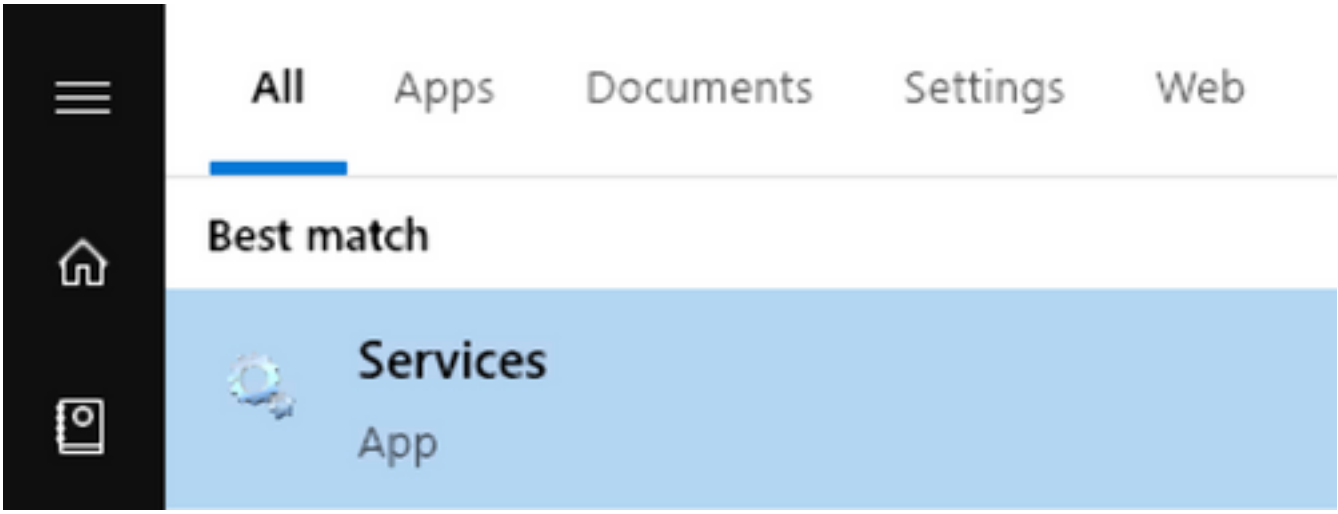
Dépanner

Le contournement de cette bogue est de retarder le service windows qui commence avant le service d'AMP.

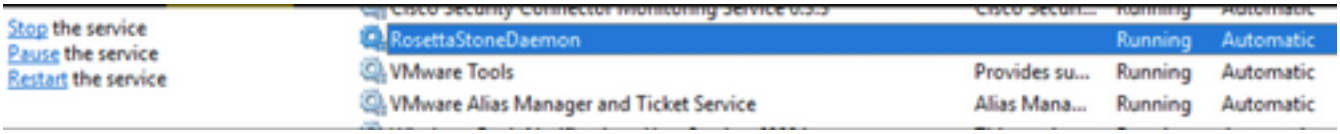
L'application de pierre de Rosetta est prise comme exemple dans ce document. Cette application est détectée par des espèces parce qu'elle touche le processus lsass.exe pour l'authentification.

Étapes pour retarder un service windows

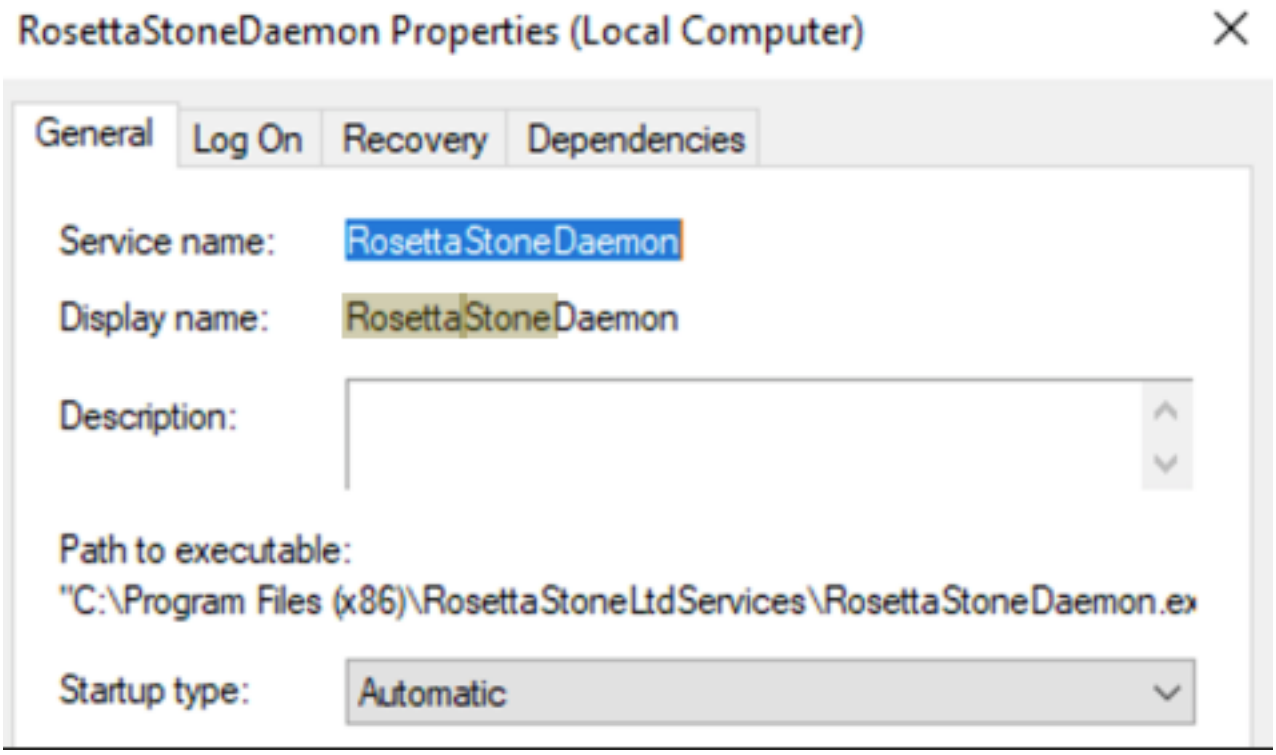
Étape 1. Ouvrez services.msc, suivant les indications de l'image.



Étape 2. Service de pierre de Rosetta de découverte.

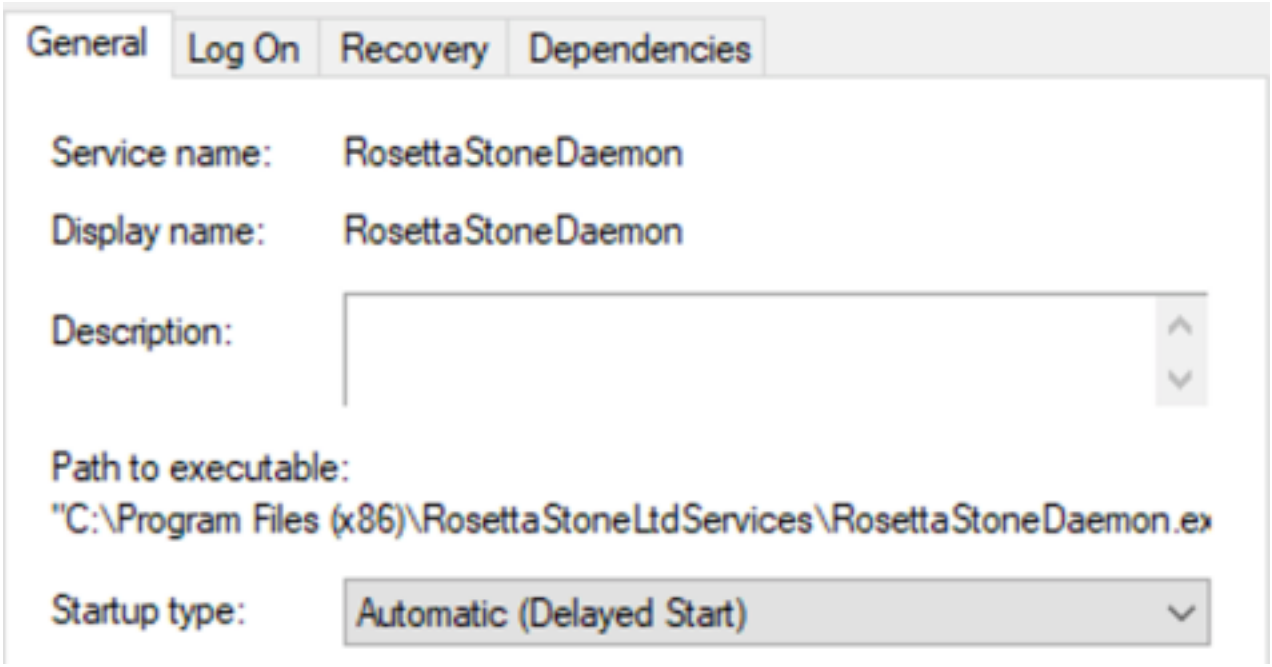


Étape 3. Le clic droit sur RosettaStoneDaemon et cliquent sur en fonction Properties.



Le type de démarrage est configuré pendant qu'automatique par défaut qui signifie des débuts de RossettaStoneDaemon automatiquement dans le processus de démarrage.

Étape 4. Cliquez sur en fonction le menu déroulant et l'automatique choisi (début retardé).



Cette configuration empêche les débuts de service de RosettaStoneDaemon avant le connecteur d'AMP.

Étape 5. Cliquez sur s'appliquent en fonction.

Retardez le processus avec la ligne de commande

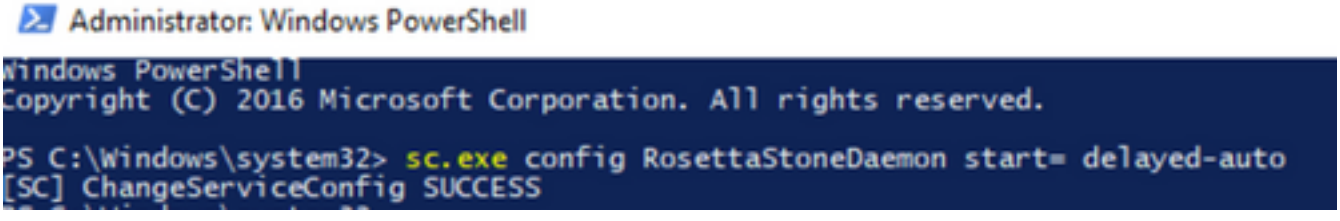
Pour PowerShell/CMD, les prochaines commandes peuvent être utilisées.

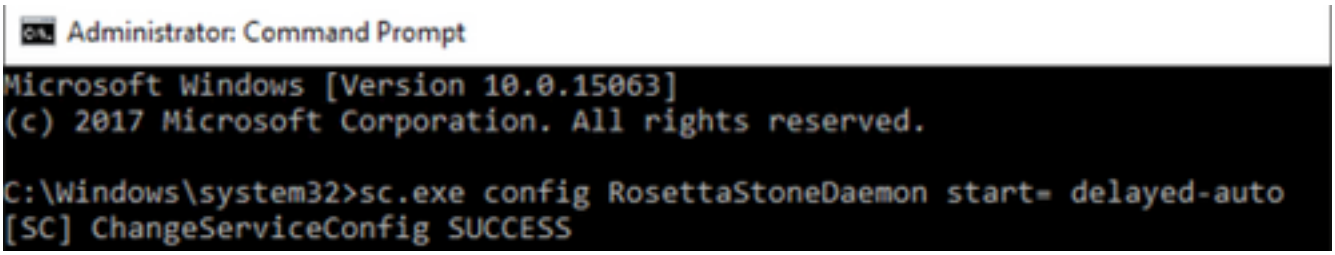
Étape 1. Exécutez PowerShell/CMD comme administrateur.

Étape 2. Exécutez cette commande :

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

Remarque: Pierre = RosettaStoneDaemon de Rosetta.





Dans cette section, vous pouvez remplacer le nom d'application de RosettaStoneDaemon pour le processus que vous voulez retarder.

> **Attention** : Version 7.0.5 de connecteur et déjà mise en place en avant une solution pour cette bogue. Ce contournement est destiné pour le soufflet 7.0.5 de versions de connecteur.