Windows Process viene avviato prima della soluzione AMP Connector - AMP for Endpoints

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi in Advanced Malware Protection (AMP) for Endpoints quando un processo Windows viene avviato prima di System Process Protection (SPP).

Contributo di Nancy Perez e Uriel Torres, tecnici Cisco TAC.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Sistema operativo Windows
- Motori del connettore AMP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- dispositivo Windows 10
- AMP connector versione 6.2.9

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Limitazioni

Si tratta di un bug che interessa il motore di Protezione processo di sistema quando un processo viene avviato prima del connettore AMP CSCvo90440.

Premesse

Il motore di protezione dei processi di sistema di AMP for Endpoints protegge i processi critici di sistema Windows dagli attacchi di aggiunta di memoria da parte di altri processi.

Per abilitare SPP, sulla console AMP, selezionare **Gestione > Criteri >** *fare clic su Modifica nella regola che si desidera modificare* **> Modi e motori > Protezione processo di sistema,** qui è possibile trovare tre opzioni:

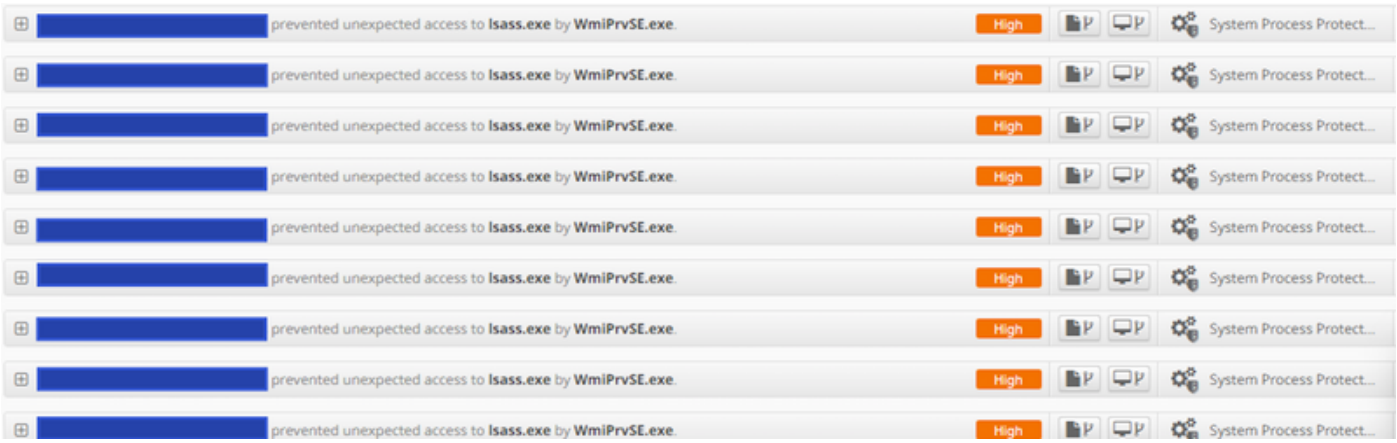
- Protezione: blocca gli attacchi ai processi critici di Windows
- Controllo: notificare gli attacchi ai processi critici di Windows
- Disattivato: il motore non è attivo in questa modalità

Processi di sistema protetti

Il motore di protezione dei processi di sistema protegge i processi successivi:

- Sottosistema di gestione delle sessioni (**smss.exe**)
- Sottosistema di runtime client/server (**csrss.exe**)
- Sottosistema autorità di sicurezza locale (**lsass.exe**)
- Applicazione di accesso a Windows (**winlogon.exe**)
- Applicazione di avvio di Windows (**wininit.exe**)

Quando un servizio Windows viene avviato prima che il connettore AMP (nelle versioni precedenti alla 7.0.5) le esclusioni dei processi di sistema non vengano rispettate e anche se un processo viene escluso, il motore SPP interrompe il processo e nella console AMP viene creato un evento, come mostrato nell'immagine.



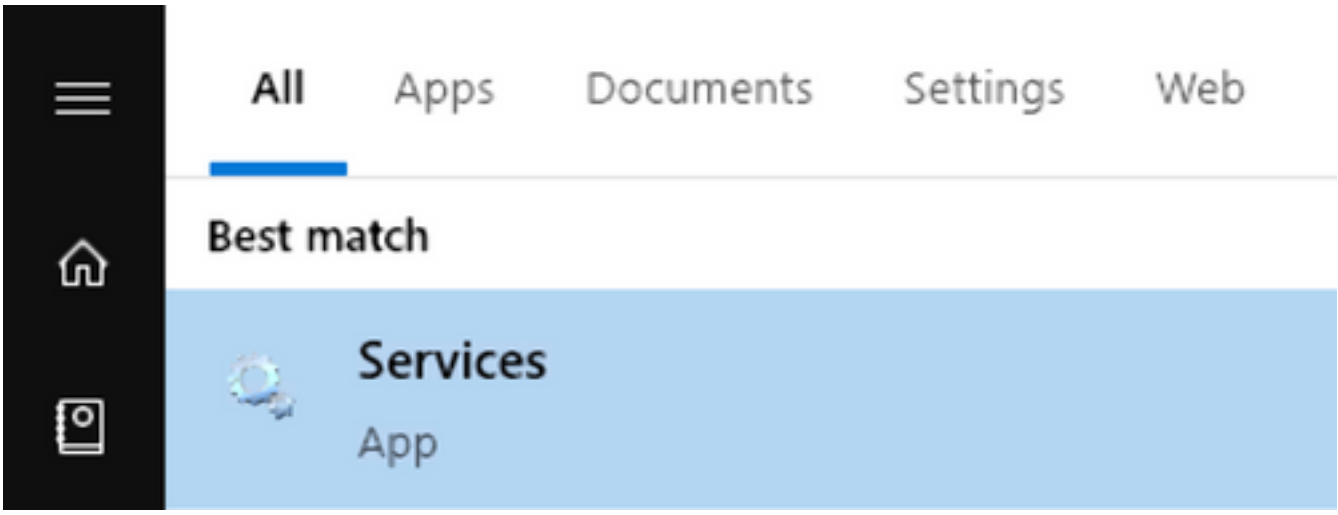
Risoluzione dei problemi

Per risolvere questo bug, è necessario ritardare l'avvio del servizio Windows prima dell'avvio del servizio AMP.

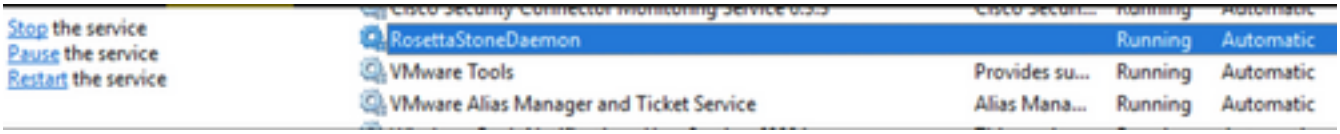
L'applicazione Rosetta Stone è presa come esempio in questo documento. Questa applicazione viene rilevata da SPP perché tocca il processo lsass.exe a scopo di autenticazione.

Passaggi per ritardare un servizio Windows

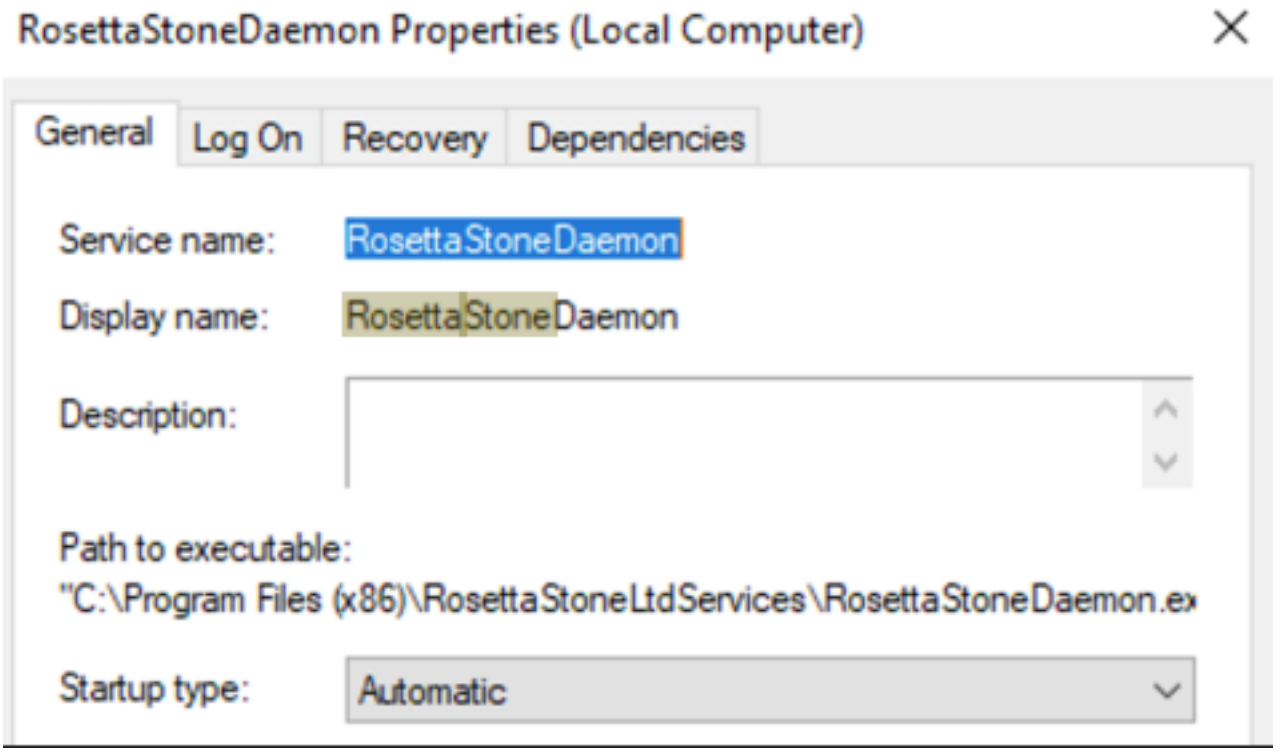
Passaggio 1. Aprire services.msc, come illustrato nell'immagine.



Passaggio 2. Trovare Rosetta Stone servizio.

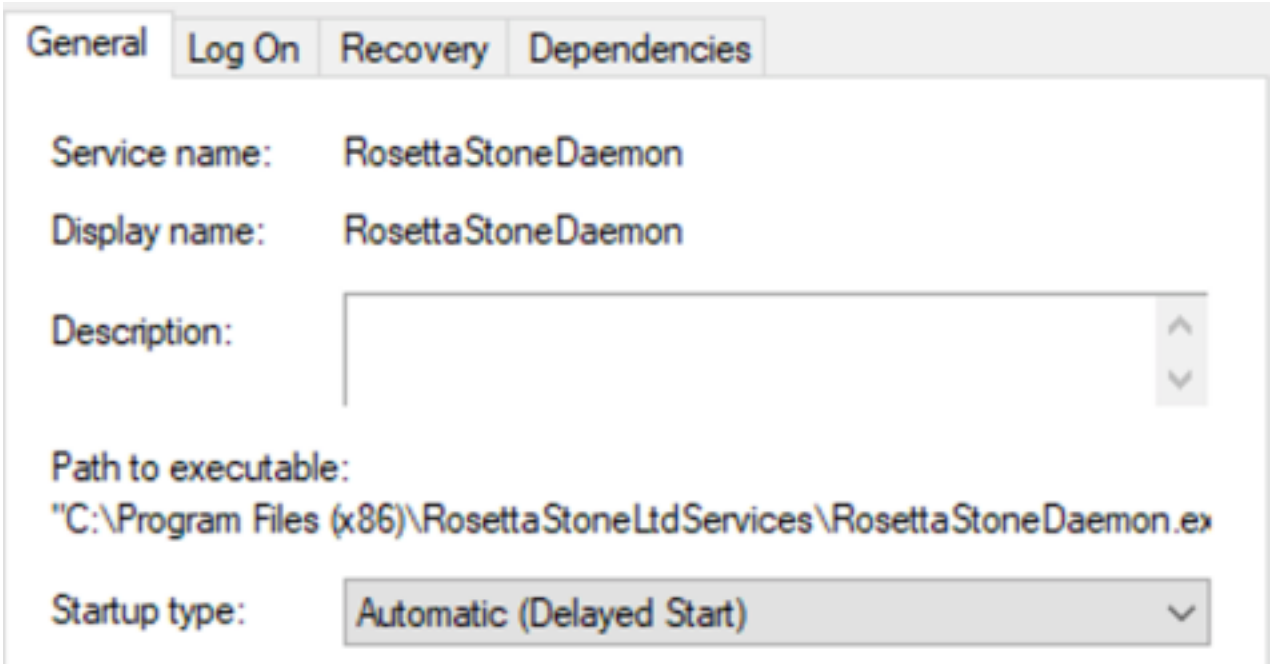


Passaggio 3. Fare clic con il pulsante destro del mouse su RosettaStoneDaemon e selezionare Proprietà.



Il tipo di avvio è configurato come Automatico per impostazione predefinita, il che significa che RossettaStoneDaemon si avvia automaticamente nel processo di avvio.

Passaggio 4. Fare clic sul menu a discesa e selezionare Automatico (avvio ritardato).



Questa configurazione impedisce l'avvio del servizio RosettaStoneDaemon prima del connettore AMP.

Passaggio 5. Fare clic su Applica.

Ritardare il processo con la riga di comando

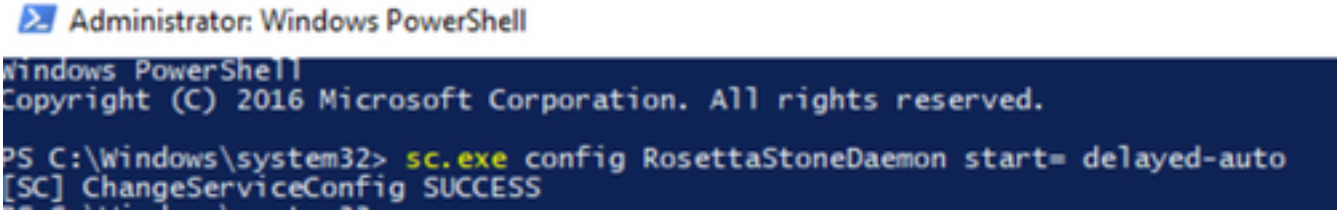
Per PowerShell/CMD è possibile utilizzare i comandi successivi.

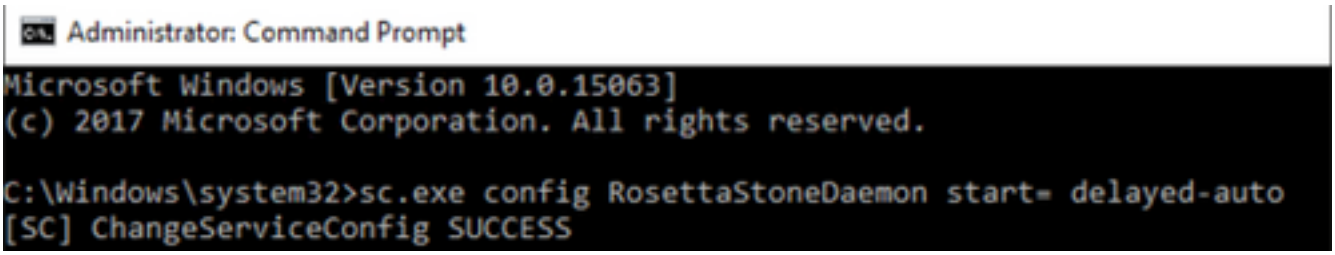
Passaggio 1. Eseguire PowerShell/CMD come amministratore.

Passaggio 2. Eseguire questo comando:

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

Nota: Rosetta Stone = RosettaStone Daemon.





In questa sezione, è possibile sostituire il nome applicazione di RosettaStoneDaemon per il processo che si desidera ritardare.

> **Attenzione**: Connector versione 7.0.5 e successive implementa già una soluzione per questo bug. Questa soluzione è destinata alle versioni dei connettori inferiori a 7.0.5.