

Scénario d'entraînement - Injection de processus

Nom du groupe

Données d'entraînement - Injection de processus (Hive)

Scénario

Dans ce scénario d'entraînement, nous allons exécuter une charge utile de rançongiciel via une injection de processus dans un Svchost.exe déjà en cours d'exécution. Le Svchost en question est une opération système normale, en cours d'exécution depuis longtemps, signée, et sous le compte utilisateur LocalSystem.

Parce que le Svchost est « réel », il est souvent négligé. Les administrateurs savent que de nombreuses instances de Svchost sont exécutées, et tant que les arguments du programme semblent corrects, il est traité comme une « boîte noire » et laissé tranquille. Il s'agit d'une faille évidente, et souvent exploitée, dont les pirates tirent parti. Combinée à une charge utile de type zero-day, cette approche est très efficace pour dissimuler les attaques de rançongiciels.

L'identifier

Number of Incidents	Machine Name	Program Path	Program Arguments
▼ 1	\\CC-NOAH-TEST	C:\Windows\System32\svchost.exe	-k UnistackSvcGroup

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 9:16:41 PM EDT	 Royal-purple Komc	True	False	False



La situation autour de cette réponse automatisée n'est pas directement apparente à première vue. Les arguments de ligne de commande semblent valides pour Svchost, et l'exécutable est signé par Microsoft.

Le fait qu'il y ait un thread distant non fiable est suspect, mais nécessite une investigation plus approfondie. De nombreux threads distants se produisent sur un système, mais la plupart restent « fiables » car ils sont utilisés pour la communication inter-processus normale, le partage de données, etc.

C'est lorsqu'un thread distant est créé dans un processus de manière anormale, et qu'il est marqué comme non fiable, que nous devons examiner cela de plus près.

Injector Pid	Injector Path	Injectee Pid	Injectee Path ↑
3992	C:\Windows\System32\csrss.exe	8844	C:\Windows\System32\cmd.exe
4228	C:\Windows\System32\dwm.exe	3992	C:\Windows\System32\csrss.exe
3268	C:\Windows\System32\dwm.exe	5972	C:\Windows\System32\csrss.exe
4228	C:\Windows\System32\dwm.exe	3992	C:\Windows\System32\csrss.exe

Injections de processus innocentes qui se produisent normalement

Afin de trier les nombreuses injections de processus qui se produisent sur un système à un moment donné, nous pouvons nous référer à la fois à l'heure de l'incident et au pid du processus signalé. Normalement, nous commencerons avec quelques pids de réponses suspectes, et remonterons la chaîne des injections et des créations pour obtenir l'histoire complète.

Response Details



Description	Value
Response Name	Royal-purple Komodo-Dragon Lavender 848
Machine Name	\\CC-NOAH-TEST
Program Path	C:\Windows\System32\svchost.exe
Program Arguments	-k UnistackSvcGroup
Agent Name	
Ram usage	0
File access count	0
Number of threads	0
Pid	6224

[View Certificate Publisher Names](#)

Injectee Pid ▼

6224

≡

▼

☰

Equals ▼

6224

Reset

Apply

Filtrage des injections non pertinentes

Injector Pid	Injector Path	Injectee Pid ▼	Injectee Path ↑
9168	C:\svchost_injector.exe	6224	C:\Windows\System32\svchost.exe

La preuve irréfutable !

Nous savons déjà que personne ne devrait injecter dans Svchost de cette manière, mais certainement pas ce processus ! À partir de maintenant, nous pouvons traiter ce processus comme s'il s'agissait de « malware.exe » et voir qui l'a exécuté, puisque quelqu'un a dû le faire.

Created ↑	Child Pid ▾	Parent Path	Child Path
October 18, 2022 at 9:11:09 PM EDT	9168	C:\Windows\System32\services.exe	C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
October 18, 2022 at 9:16:04 PM EDT	9168	C:\Windows\explorer.exe	C:\svchost_injector.exe

Processus démarrés avec le pid 9168

Puisqu'il y a eu deux créations de processus avec le pid 9168, et qu'elles sont très différentes, nous pouvons affiner en fonction de l'horodatage et/ou du chemin enfant, et constater que cela a été créé par un explorer.exe. Cela signifie que quelqu'un a manuellement exécuté le processus d'injection, et il ne peut s'agir d'une coïncidence de comportement de Svchost qui aurait été signalé à tort.

Documentation pertinente

- **Injection de processus**

- [Mitre T1559](#) - La communication inter-processus peut fournir un contrôle sur le processus cible depuis l'injecteur une fois l'injection terminée.
- [Mitre T1106](#) - Les API natives constituent souvent l'accès le plus direct aux fonctionnalités du système d'exploitation pour accéder aux fichiers, exécuter des processus, et plus encore.
- [Mitre T1569](#) - Injecter dans un service système tel qu'un svchost existant peut déguiser du code malveillant pour qu'il soit signalé comme s'exécutant à partir d'un processus bien connu et fiable.
- [Mitre T1055](#) - L'injection de processus, généralement utilisée pour exécuter du code malveillant dans un processus cible tout en permettant au processus d'origine de continuer.

Revision #1

Created 2026-07-24 06:21:14 UTC by Dennis Underwood

Updated 2026-07-24 06:21:15 UTC by Dennis Underwood