Cenário de Treinamento - Injeção de Processo

Nome do Grupo

Dados de Treinamento - Injeção de Processo (Hive)

Cenário

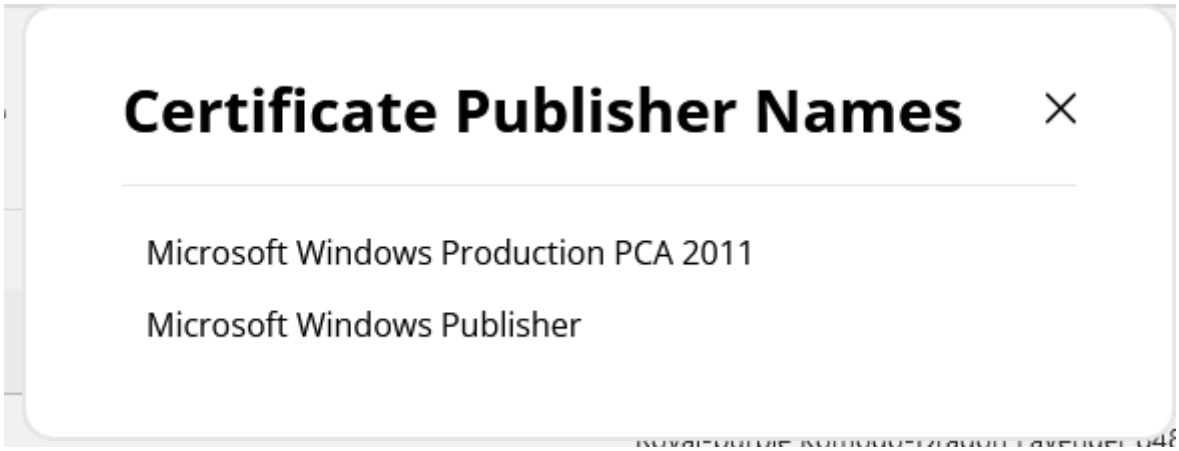
Neste cenário de treinamento, executaremos uma carga útil de ransomware por meio de injeção de processo em um Svchost.exe já em execução. O Svchost em questão é uma operação normal do sistema, em execução há muito tempo, assinado e sob a conta de usuário LocalSystem.

Como o Svchost é ‘real’, ele é frequentemente ignorado. Os administradores sabem que muitas instâncias do Svchost são executadas, e desde que os argumentos do programa pareçam corretos, ele é tratado como uma “caixa preta” e deixado de lado. Esta é uma brecha óbvia, e frequentemente explorada, para que hackers tirem vantagem. Combinada com uma carga útil de dia zero, essa abordagem é muito bem-sucedida em ofuscar ataques de ransomware.

Identificando-o

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



Assinante(s) do Certificado do svchost.exe

A situação em torno dessa resposta automatizada não é diretamente aparente à primeira vista. Os argumentos de linha de comando parecem válidos para o Svchost, e o executável é assinado pela Microsoft.

O fato de haver uma thread remota não confiável é suspeito, mas requer mais investigação. Muitas threads remotas acontecem em um sistema, mas a maioria permanece “confiável”, pois são usadas para comunicação normal entre processos, compartilhamento de dados, etc.

Quando uma thread remota é criada em um processo de forma anormal, e é marcada como não confiável, é onde precisamos examinar com mais rigor.

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

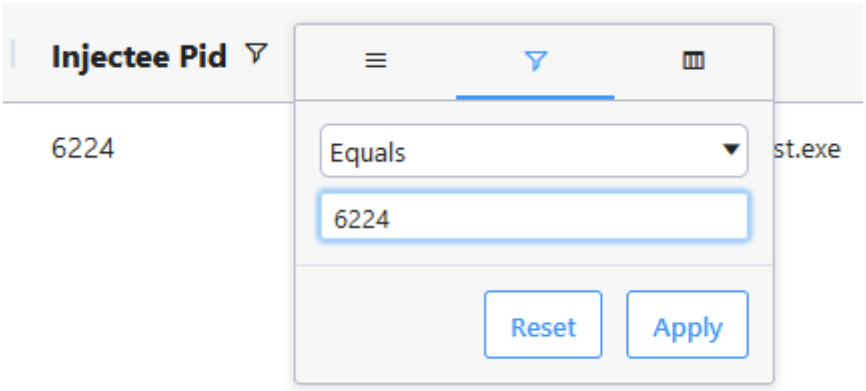
Injeções de Processo Inocentes que ocorrem normalmente

Para filtrar as muitas injeções de processo que ocorrem em um sistema a qualquer momento, podemos nos referir tanto ao horário do incidente quanto ao pid do processo sinalizado. Normalmente, começaremos com alguns pids de respostas suspeitas e subiremos na cadeia de injeções e criações para obter a história completa.

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



Filtrando injeções irrelevantes

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

A prova irrefutável!

Já sabemos que ninguém deveria estar injetando no Svchost dessa maneira, mas definitivamente não este processo! A partir daqui, podemos tratar esse processo como se fosse “malware.exe” e ver quem o executou, já que alguém deve tê-lo feito.

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

Processos iniciados com pid 9168

Como houve duas criações de processo com pid 9168, e elas são muito diferentes, podemos restringir com base no timestamp e/ou no caminho do processo filho, e ver que foi criado por um explorer.exe. Isso significa que alguém executou manualmente o processo injetor, e não pode ser uma coincidência de comportamento do Svchost sinalizado incorretamente.

Documentação relevante

- **Injeção de Processo**
- Mitre T1559 - A comunicação entre processos pode fornecer controle sobre o processo alvo a partir do injetor uma vez que a injeção esteja concluída.
- Mitre T1106 - As APIs nativas são frequentemente o acesso mais próximo à funcionalidade do sistema operacional para acessar arquivos, executar processos e mais.
- Mitre T1569 - Injetar em um serviço do sistema como um svchost existente pode disfarçar código malicioso para ser reportado como sendo executado a partir de um processo bem conhecido e confiável.
- Mitre T1055 - Injeção de processo, geralmente usada para executar código malicioso em um processo alvo enquanto permite que o processo original continue.

Revision #1
Created 2026-07-24 05:12:55 UTC by Dennis Underwood
Updated 2026-07-24 05:12:55 UTC by Dennis Underwood