Injeção de Processo

O que são injeções de processo?

Injeções de processo ocorrem quando um processo A (potencialmente malicioso) força um processo B a executar instruções que de outra forma não fazem parte do seu código. A injeção de processo possui muitas técnicas diferentes, sendo a mais comum a criação de uma thread remota dentro do processo vítima.

Frequentemente, essas novas instruções são criadas lado a lado com o programa original, de modo que as operações normais do processo vítima B não sejam afetadas. Por causa disso, a injeção muitas vezes passa despercebida.

Táticas relevantes do Mitre:

- Mitre T1055 - Injeção de processo, conforme descrito acima. Usada para evadir a detecção de malware, permitindo que o processo alvo continue operando normalmente enquanto executa código malicioso.
- Mitre T1559 - A comunicação entre processos (Inter-Process communication) pode fornecer controle sobre o processo alvo a partir do injetor, uma vez concluída a injeção.
- Mitre T1569 - Injetar em um serviço do sistema, como um `svchost` existente, pode disfarçar código malicioso para que ele seja reportado como sendo executado a partir de um processo conhecido e confiável.

Quais são as consequências?

Injeções de processo não confiáveis em um processo que de outra forma seria confiável significam que ele deixa de ser confiável. Uma instalação não corrompida de software seguro, como um servidor SQL, pode ser forçada a executar cargas úteis de malware. Após a morte do processo e/ou a reinicialização do sistema, qualquer evidência dessa violação desaparecerá, já que tudo foi feito puramente em memória com criação dinâmica de threads.

O que a Cyber Crucible faz?

A Cyber Crucible monitora as injeções de processo que ocorrem no sistema e não interrompe a atividade, a menos que atividades de extorsão de dados ou criptografia de ransomware tenham

começado. Isso ocorre porque alguns processos no sistema se comunicam por meio de diferentes técnicas de injeção de processo e não realizam nenhum comportamento malicioso.

Em vez disso, a Cyber Crucible acompanha as injeções que ocorrem de e para cada processo no sistema, registrando-as para uso posterior em uma possível análise de causa raiz. Dessa forma, podemos saber não apenas que um determinado processo está atualmente não confiável em memória, mas também qual processo iniciou a cadeia de atividade maliciosa.

Como posso saber?

31784977.png?width=510
Quando uma resposta automatizada tem o campo “untrusted remote threads” definido como verdadeiro, sabemos que estamos lidando com injeções de processo. A boa notícia é que podemos obter o pid da resposta e pesquisar as injeções de processo em torno do momento do incidente, encontrando o responsável.

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

Cenários de exemplo:

- Cenário de Treinamento - Injeção de Processo

Revision #1
Created 2026-07-24 05:10:58 UTC by Dennis Underwood
Updated 2026-07-24 05:10:58 UTC by Dennis Underwood