Injection de processus

Qu'est-ce que l'injection de processus ?

L'injection de processus se produit lorsqu'un processus A (potentiellement malveillant) force un processus B à exécuter des instructions qui ne font pas partie de son code. L'injection de processus comprend de nombreuses techniques différentes, la plus courante consistant à créer un thread distant à l'intérieur du processus victime.

Souvent, ces nouvelles instructions sont créées parallèlement au programme original, de sorte que les opérations normales du processus victime B ne sont pas affectées. Pour cette raison, l'injection passe souvent inaperçue.

Tactiques Mitre pertinentes :

- Mitre T1055 - Injection de processus, comme décrit ci-dessus. Utilisée pour échapper à la détection de logiciels malveillants en permettant au processus cible de continuer à fonctionner normalement tout en exécutant du code malveillant.
- Mitre T1559 - La communication inter-processus peut permettre de prendre le contrôle du processus cible depuis l'injecteur une fois l'injection terminée.
- Mitre T1569 - Injecter dans un service système tel qu'un `svchost` existant peut déguiser le code malveillant pour qu'il soit signalé comme provenant d'un processus connu et fiable.

Quelles sont les conséquences ?

L'injection de processus non fiables dans un processus par ailleurs fiable signifie que celui-ci n'est plus fiable. Une installation par ailleurs non corrompue d'un logiciel sécurisé, comme un serveur SQL, peut être forcée à exécuter des charges utiles malveillantes. Après la mort du processus et/ou le redémarrage du système, toute preuve de cette altération disparaîtra, car tout a été effectué purement en mémoire avec une création dynamique de threads.

Que fait Cyber Crucible ?

Cyber Crucible surveille les injections de processus qui se produisent sur le système, et n'arrête pas l'activité sauf si des activités d'extorsion de données ou de chiffrement par rançongiciel ont commencé. Cela s'explique par le fait que certains processus du système communiquent via

différentes techniques d'injection de processus, sans effectuer de comportement malveillant.

Au lieu de cela, Cyber Crucible gardera une trace des injections qui se produisent vers et depuis chaque processus sur le système, et les enregistrera en vue d'une éventuelle analyse des causes profondes ultérieure. Ainsi, nous pouvons savoir non seulement qu'un processus particulier n'est actuellement pas fiable en mémoire, mais aussi quel processus a déclenché la chaîne d'activité malveillante.

Comment le savoir ?

31784977.png?width=510
Lorsqu'une réponse automatisée a le champ « untrusted remote threads » à vrai, nous savons que nous avons affaire à des injections de processus. La bonne nouvelle est que nous pouvons récupérer le pid de la réponse, et parcourir les injections de processus autour du moment de l'incident, pour trouver le coupable.

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

Exemples de scénarios :

- Scénario de formation - Injection de processus

Revision #1
Created 2026-07-24 06:19:06 UTC by Dennis Underwood
Updated 2026-07-24 06:19:06 UTC by Dennis Underwood