Inyección de Procesos

¿Qué son las inyecciones de procesos?

Las inyecciones de procesos ocurren cuando un proceso A (potencialmente malicioso) obliga al proceso B a ejecutar instrucciones que de otro modo no formarían parte de su código. La inyección de procesos cuenta con muchas técnicas diferentes, siendo la más común la creación de un hilo remoto dentro del proceso víctima.

A menudo, estas nuevas instrucciones se crean junto al programa original, de modo que las operaciones normales del proceso víctima B no se ven afectadas. Debido a esto, la inyección a menudo pasa desapercibida.

Tácticas relevantes de Mitre:

- Mitre T1055 - Inyección de procesos, como se describió anteriormente. Se utiliza para evadir la detección de malware, permitiendo que el proceso objetivo continúe operando normalmente mientras ejecuta código malicioso.
- Mitre T1559 - La comunicación entre procesos puede proporcionar control sobre el proceso objetivo por parte del inyector una vez completada la inyección.
- Mitre T1569 - Inyectar en un servicio del sistema, como un `svchost` existente, puede disfrazar el código malicioso para que se reporte como ejecutándose desde un proceso conocido y de confianza.

¿Cuáles son las consecuencias?

Las inyecciones de procesos no confiables en un proceso que de otro modo sería confiable implican que este ya no lo es. Una instalación no corrupta de un software seguro, como un servidor SQL, puede verse forzada a ejecutar cargas útiles de malware. Tras la muerte del proceso y/o el reinicio del sistema, cualquier evidencia de esta manipulación desaparecerá, ya que todo se realizó puramente en memoria mediante la creación dinámica de hilos.

¿Qué hace Cyber Crucible?

Cyber Crucible monitorea las inyecciones de procesos que ocurren en el sistema, y no detiene la actividad a menos que hayan comenzado actividades de extorsión de datos o cifrado por

ransomware. Esto se debe a que algunos procesos del sistema se comunican mediante distintas técnicas de inyección de procesos, sin llevar a cabo ningún comportamiento malicioso.

En su lugar, Cyber Crucible llevará un registro de las inyecciones que ocurren hacia y desde cada proceso en el sistema, y las registrará para su uso en un posible análisis de causa raíz posteriormente. De esta manera, podemos saber no solo que un proceso en particular no es confiable actualmente en memoria, sino también qué proceso inició la cadena de actividad maliciosa.

¿Cómo puedo saberlo?

31784977.png?width=510
Cuando una respuesta automatizada tiene el campo “untrusted remote threads” (hilos remotos no confiables) en verdadero, sabemos que estamos ante una inyección de procesos. La buena noticia es que podemos obtener el pid de la respuesta, y buscar entre las inyecciones de procesos alrededor del momento del incidente, para encontrar al responsable.

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

Escenarios de ejemplo:

- Escenario de Capacitación - Inyección de Procesos

Revision #1
Created 2026-07-24 01:12:43 UTC by Dennis Underwood
Updated 2026-07-24 01:12:43 UTC by Dennis Underwood