Prozessinjektion

Was sind Prozessinjektionen?

Prozessinjektionen liegen vor, wenn ein (möglicherweise bösartiger) Prozess A einen Prozess B dazu zwingt, Anweisungen auszuführen, die andernfalls nicht Teil seines Codes wären. Für Prozessinjektionen gibt es viele verschiedene Techniken, wobei die gängigste darin besteht, einen Remote-Thread innerhalb des Zielprozesses zu erstellen.

Häufig werden diese neuen Anweisungen parallel zum ursprünglichen Programm erstellt, sodass der normale Betrieb des Zielprozesses B nicht beeinträchtigt wird. Aus diesem Grund bleibt die Injektion oft unbemerkt.

Relevante Mitre-Taktiken:

- Mitre T1055 - Prozessinjektion, wie oben beschrieben. Wird verwendet, um die Malware-Erkennung zu umgehen, indem der Zielprozess weiterhin normal arbeiten kann, während bösartiger Code ausgeführt wird.
- Mitre T1559 - Interprozesskommunikation kann nach abgeschlossener Injektion die Kontrolle über den Zielprozess vom Injector aus ermöglichen.
- Mitre T1569 - Das Einschleusen in einen Systemdienst wie einen vorhandenen `svchost` kann bösartigen Code so tarnen, dass er als von einem bekannten und vertrauenswürdigen Prozess ausgeführt gemeldet wird.

Welche Folgen hat das?

Nicht vertrauenswürdige Prozessinjektionen in einen ansonsten vertrauenswürdigen Prozess bedeuten, dass dieser nicht mehr vertrauenswürdig ist. Eine ansonsten unbeschädigte Installation gesicherter Software, wie beispielsweise ein SQL-Server, kann dazu gezwungen werden, Malware-Payloads auszuführen. Nach dem Beenden des Prozesses und/oder einem Neustart des Systems ist jeder Beweis für diese Manipulation verschwunden, da alles rein im Arbeitsspeicher mittels dynamischer Thread-Erstellung ausgeführt wurde.

Was tut Cyber Crucible?

Cyber Crucible überwacht Prozessinjektionen, die auf dem System auftreten, und stoppt die Aktivität nicht, es sei denn, es haben Datenexfiltrationsaktivitäten oder eine Ransomware-Verschlüsselung begonnen. Dies liegt daran, dass einige Prozesse auf dem System über verschiedene Prozessinjektionstechniken kommunizieren, ohne dabei bösartiges Verhalten auszuführen.

Stattdessen verfolgt Cyber Crucible die Injektionen, die zu und von jedem Prozess auf dem System stattfinden, und zeichnet sie für eine spätere mögliche Ursachenanalyse auf. Auf diese Weise können wir nicht nur erkennen, dass ein bestimmter Prozess derzeit im Arbeitsspeicher nicht vertrauenswürdig ist, sondern auch, welcher Prozess die Kette bösartiger Aktivitäten ausgelöst hat.

Wie erkenne ich das?

31784977.png?width=510
Wenn bei einer automatisierten Reaktion das Feld „untrusted remote threads“ den Wert „true“ hat, wissen wir, dass es sich um Prozessinjektionen handelt. Die gute Nachricht ist, dass wir die PID der Reaktion abrufen und die Prozessinjektionen rund um den Zeitpunkt des Vorfalls durchsuchen können, um den Verursacher zu finden.

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

Beispielszenarien:

- Schulungsszenario - Prozessinjektion

Revision #1
Created 2026-07-24 03:53:51 UTC by Dennis Underwood
Updated 2026-07-24 03:53:51 UTC by Dennis Underwood