





/Tracker.exe

☆ Star

7,060

- Execute (DLL)
- AWL bypass (DLL)

Tool included with Microsoft .Net Framework.

Paths:
no default

- Resources:**
- <https://twitter.com/subTee/status/793151392185589760>
 - <https://attack.mitre.org/wiki/Execution>

- Acknowledgements:**
- Casey Smith ([@subTee](#))

- Detections:**
- Sigma: [proc_creation_win_lolbin_tracker.yml](#)

Execute

Use tracker.exe to proxy execution of an arbitrary DLL into another process. Since tracker.exe is also signed it can be used to bypass application whitelisting solutions.

```
Tracker.exe /d .\calc.dll /c C:\Windows\write.exe
```

Use case:	Injection of locally stored DLL file into target process.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1127: Trusted Developer Utilities Proxy Execution
Tags:	Execute: DLL

AWL bypass

Use tracker.exe to proxy execution of an arbitrary DLL into another process. Since tracker.exe is also signed it can be used to bypass application whitelisting solutions.

```
Tracker.exe /d .\calc.dll /c C:\Windows\write.exe
```

Use case:	Injection of locally stored DLL file into target process.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1127: Trusted Developer Utilities Proxy Execution
Tags:	Execute: DLL