.. /Tracker.exe

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: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/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
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
Tags:	Execute: DLL