.. /Ttdinject.exe

Star 7,060

Execute

Used by Windows 1809 and newer to Debug Time Travel (Underlying call of tttracer.exe)

Paths:
C:\Windows\System32\ttdinject.exe
C:\Windows\Syswow64\ttdinject.exe

Resources:

- https://twitter.com/Oddvarmoe/status/1196333160470138880

Acknowledgements:

- Oddvar Moe (@oddvarmoe)
- Maxime Nadeau (@m_nad0)

Detections:

- Sigma: create_remote_thread_win_ttdinjec.yml
- Sigma: proc_creation_win_lolbin_ttdinject.yml
- IOC: Parent child relationship. Ttdinject.exe parent for executed command
- IOC: Multiple queries made to the IFEO registry key of an untrusted executable (Ex. "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\payload.exe") from the ttdinject.exe process

Execute

1. Execute calc using ttdinject.exe. Requires administrator privileges. A log file will be created in tmp.run. The log file can be changed, but the length (7) has to be updated.

```
TTDInject.exe /ClientParams "7 tmp.run 0 0 0 0 0 0 0 0 0 0" /Launch "C:/Windows/System32/calc.exe"
```

Use case:	Spawn process using other binary
Privileges required:	Administrator
Operating systems:	Windows 10 2004 and above, Windows 11
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution

2. Execute calc using ttdinject.exe. Requires administrator privileges. A log file will be created in tmp.run. The log file can be changed, but the length (7) has to be updated.

```
ttdinject.exe /ClientScenario TTDRecorder /ddload 0 /ClientParams "7 tmp.run 0 0 0 0 0 0 0 0 0 0" /launch "C:/Windows/System32/calc.exe"
```

Use case:	Spawn process using other binary
Privileges required:	Administrator
Operating systems:	Windows 10 1909 and below
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution