# ... /Ttdinject.exe



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 (<u>@oddvarmoe</u>)
- Maxime Nadeau (@m\_nad0)

#### **Detections:**

Sigma:

https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/create\_remote\_thread/create\_remote\_thread\_win\_ttdinjec.yml

Sigma:

https://github.com/SigmaHQ/sigma/blob/7ea6ed3db65e0bd812b051d9bb4fffd27c4c4d0a/rules/windows/process\_creation/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**

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 " /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

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.

**Use case:** Spawn process using other binary

Privileges required: Administrator

Operating systems: Windows 10 1909 and below

ATT&CK® technique: T1127