.. /Tttracer.exe

Star 7,060

Execute Dump

Used by Windows 1809 and newer to Debug Time Travel

Paths:
C:\Windows\System32\tttracer.exe
C:\Windows\SysWOW64\tttracer.exe

Resources:

- https://twitter.com/oulusoyum/status/1191329746069655553
- https://twitter.com/mattifestation/status/1196390321783025666
- https://lists.samba.org/archive/cifs-protocol/2016-April/002877.html

Acknowledgements:

- Onur Ulusoy (@oulusoyum)
- Matt Graeber (@mattifestation)

Detections:

- Sigma: proc_creation_win_lolbin_tttracer_mod_load.yml
- Sigma: image_load_tttracer_mod_load.yml
- Elastic: credential_access_cmdline_dump_tool.toml
- IOC: Parent child relationship. Tttracer parent for executed command

Execute

Execute calc using tttracer.exe. Requires administrator privileges

```
tttracer.exe C:\windows\system32\calc.exe
```

Use case:	Spawn process using other binary
Privileges required:	Administrator
Operating systems:	Windows 10 1809 and newer, Windows 11
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution

Dump

Dumps process using tttracer.exe. Requires administrator privileges

```
TTTracer.exe -dumpFull -attach pid
```

Use case:	Dump process by PID
Privileges required:	Administrator
Operating systems:	Windows 10 1809 and newer, Windows 11
ATT&CK® technique:	**T1003**: OS Credential Dumping