.. /Tttracer.exe

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: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_tttracer_mod_load.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/image_load/image_load_tttracer_mod_load.yml
- Elastic: https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/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

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