.. /Dxcap.exe

Execute

DirectX diagnostics/debugger included with Visual Studio.

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

Resources:
- https://twitter.com/harr0ey/status/992008180904419328

Acknowledgements:
- Matt harr0ey (@harr0ey)
- Vikas Singh (@vikas891)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_susp_dxcap.yml

Execute

Launch notepad.exe as a subprocess of dxcap.exe. Note that you should have write permissions in the current working directory for the command to succeed; alternatively, add '-file c:\path\to\writable\location.ext' as first argument.

```
Dxcap.exe -c C:\Windows\System32\notepad.exe
```

Use case: Local execution of a process as a subprocess of dxcap.exe
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1127