.. /Verclsid.exe

☆ Star 7,060

Execute

Used to verify a COM object before it is instantiated by Windows Explorer

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

Resources:

- https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5
- https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/

Acknowledgements:

- Nick Tyrer (@NickTyrer)

Detections:

- Sigma: proc_creation_win_verclsid_runs_com.yml
- Splunk: verclsid_clsid_execution.yml

Execute

Used to verify a COM object before it is instantiated by Windows Explorer

```
verclsid.exe /S /C {CLSID}
```

Use case:	Run a com object created in registry to evade defensive counter measures
Privileges required:	User
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	**T1218.012**: Verclsid