.. /Register-cimprovider.exe ☆ Star

Execute (DLL)

Used to register new wmi providers

Paths:
C:\Windows\System32\Register-cimprovider.exe
C:\Windows\SysWOW64\Register-cimprovider.exe

Resources:
- https://twitter.com/PhilipTsukerman/status/992021361106268161

Acknowledgements:
- Philip Tsukerman (@PhilipTsukerman)

Detections:
- Sigma: proc_creation_win_susp_register_cimprovider.yml
- IOC: Register-cimprovider.exe execution and cmdline DLL load may be supsicious

Execute

Load the target .DLL.

```
Register-cimprovider -path "C:\folder\evil.dll"
```

Use case:	Execute code within dll file
Privileges required:	User
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1218: System Binary Proxy Execution
Tags:	Execute: DLL