.. /UtilityFunctions.ps1

☆ Star 7,060

Execute (DLL)

PowerShell Diagnostic Script

Paths:
C:\Windows\diagnostics\system\Networking\UtilityFunctions.ps1

Resources:

- https://twitter.com/nickvangilder/status/1441003666274668546

Acknowledgements:

- Nick VanGilder (@nickvangilder)

Detections:

- Sigma: proc_creation_win_lolbas_utilityfunctions.yml

Execute

Proxy execute Managed DLL with PowerShell

```
powershell.exe -ep bypass -command "set-location -path c:\windows\diagnostics\system\networking; import-module
.\UtilityFunctions.ps1; RegSnapin ..\..\..\..\temp\unsigned.dll;[Program.Class]::Main()"
```

Use case:	Execute proxied payload with Microsoft signed binary
Privileges required:	User
Operating systems:	Windows 10 21H1 (likely other versions as well), Windows 11
ATT&CK® technique:	**T1216**: System Script Proxy Execution
Tags:	Execute: DLL