.. /Gpscript.exe ☆ Star

Execute

Used by group policy to process scripts

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

Resources:
- https://oddvar.moe/2018/04/27/gpscript-exe-another-lolbin-to-the-list/

Acknowledgements:
- Oddvar Moe (@oddvarmoe)

Detections:
- Sigma: proc_creation_win_lolbin_gpscript.yml
- IOC: Scripts added in local group policy
- IOC: Execution of Gpscript.exe after logon

Execute

1. Executes logon scripts configured in Group Policy.

```
Gpscript /logon
```

Use case:	Add local group policy logon script to execute file and hide from defensive counter measures
Privileges required:	Administrator
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1218: System Binary Proxy Execution

2. Executes startup scripts configured in Group Policy

```
Gpscript /startup
```

Use case:	Add local group policy logon script to execute file and hide from defensive counter measures
Privileges required:	Administrator
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1218: System Binary Proxy Execution