.. /Gpscript.exe

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: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_gpscript.yml
- IOC: Scripts added in local group policy
- IOC: Execution of Gpscript.exe after logon

Execute

. 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

. 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