



/Provlaunch.exe Star

Execute

Launcher process

Paths:

c:\windows\system32\provlaunch.exe

Resources:

- <https://twitter.com/0gtweet/status/1674399582162153472>

Acknowledgements:

- Grzegorz Tworek ([@0gtweet](#))

Detections:

- Sigma: [proc_creation_win_provlaunch_potential_abuse.yml](#)
- Sigma: [proc_creation_win_provlaunch_susp_child_process.yml](#)
- Sigma: [proc_creation_win_registry_provlaunch_provisioning_command.yml](#)
- Sigma: [registry_set_provisioning_command_abuse.yml](#)
- IOC: c:\windows\system32\provlaunch.exe executions
- IOC: Creation/existence of HKLM\SOFTWARE\Microsoft\Provisioning\Commands subkeys

Execute

Executes command defined in the Registry. Requires 3 levels of the key structure containing some keywords. Such keys may be created with two reg.exe commands, e.g. "reg.exe add HKLM\SOFTWARE\Microsoft\Provisioning\Commands\LOLBin\dummy1 /v altitude /t REG_DWORD /d 0" and "reg add HKLM\SOFTWARE\Microsoft\Provisioning\Commands\LOLBin\dummy1\dummy2 /v Commandline /d calc.exe". Registry keys are deleted after successful execution.

provlaunch.exe LOLBin

Use case: Executes arbitrary command

Privileges required: Administrator

Operating systems: Windows 10, Windows 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022

ATT&CK® technique: [T1218: System Binary Proxy Execution](#)