.. /Runscripthelper.exe

Execute

Execute target PowerShell script

Paths:
C:\Windows\WinSxS\amd64_microsoft-windows-u..ed-telemetry-client_31bf3856ad364e35_10.0.16299.15_none_c2df1bba78111118\Runscripthelper.exe
C:\Windows\WinSxS\amd64_microsoft-windows-u..ed-telemetry-client_31bf3856ad364e35_10.0.16299.192_none_ad4699b571e00c4a\Runscripthelper.exe

Resources:

- https://posts.specterops.io/bypassing-application-whitelisting-with-runscripthelper-exe-1906923658fc

Acknowledgements:

- Matt Graeber (@mattifestation)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_runscripthelper.yml
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- IOC: Event 4014 - Powershell logging
- IOC: Event 400

Execute

Execute the PowerShell script named test.txt

```
runscripthelper.exe surfacecheck \\?\C:\Test\Microsoft\Diagnosis\scripts\test.txt C:\Test
```

Use case:	Bypass constrained language mode and execute Powershell script
Privileges required:	User
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
ATT&CK® technique:	T1218