



/CL_Invocation.ps1 Star

Execute

Aero diagnostics script

Paths:

C:\Windows\diagnostics\system\AERO\CL_Invocation.ps1
C:\Windows\diagnostics\system\Audio\CL_Invocation.ps1
C:\Windows\diagnostics\system\WindowsUpdate\CL_Invocation.ps1

Acknowledgements:

- Jimmy ([@bohops](#))
- Pierre-Alexandre Braeken ([@pabraeken](#))

Detections:

- Sigma: [proc_creation_win_lolbin_cl_invocation.yml](#)
- Sigma: [posh_ps_cl_invocation_lolscript.yml](#)

Execute

Import the PowerShell Diagnostic CL_Invocation script and call SyncInvoke to launch an executable.

```
. C:\Windows\diagnostics\system\AERO\CL_Invocation.ps1    \nSyncInvoke <executable> [args]
```

Use case: Proxy execution
Privileges required: User
Operating systems: Windows 10
ATT&CK® technique: [T1216: System Script Proxy Execution](#)