



/CL_Mutexverifiers.ps1 Star

Execute

Proxy execution with CL_Mutexverifiers.ps1

Paths:

C:\Windows\diagnostics\system\WindowsUpdate\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\Audio\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\WindowsUpdate\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\Video\CL_Mutexverifiers.ps1
C:\Windows\diagnostics\system\Speech\CL_Mutexverifiers.ps1

Resources:

- <https://twitter.com/pabraeken/status/995111125447577600>

Acknowledgements:

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

Detections:

- Sigma: [proc_creation_win_lolbin_cl_mutexverifiers.yml](#)

Execute

Import the PowerShell Diagnostic CL_Mutexverifiers script and call runAfterCancelProcess to launch an executable.

```
. C:\Windows\diagnostics\system\AERO\CL_Mutexverifiers.ps1 \nrunAfterCancelProcess calc.ps1
```

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