.. /AccCheckConsole.exe

Execute (DLL) AWL bypass (DLL)

Verifies UI accessibility requirements

Paths:
C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x86\AccChecker\AccCheckConsole.exe
C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x64\AccChecker\AccCheckConsole.exe
C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm\AccChecker\AccCheckConsole.exe
C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm64\AccChecker\AccCheckConsole.exe

Resources:

- https://gist.github.com/bohops/2444129419c8acf837aedda5f0e7f340
- https://twitter.com/bohops/status/1477717351017680899

Acknowledgements:

- Jimmy (@bohops)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_lolbin_susp_acccheckconsole.yml
- IOC: Sysmon Event ID 1 - Process Creation
- Analysis: https://gist.github.com/bohops/2444129419c8acf837aedda5f0e7f340

Execute

Load a managed DLL in the context of AccCheckConsole.exe. The -window switch value can be set to an arbitrary active window name.

```
AccCheckConsole.exe -window "Untitled - Notepad" C:\path\to\your\lolbas.dll
```

Use case:	Local execution of managed code from assembly DLL.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1218
Tags:	Execute: DLL

AWL bypass

Load a managed DLL in the context of AccCheckConsole.exe. The -window switch value can be set to an arbitrary active window name.

```
AccCheckConsole.exe -window "Untitled - Notepad" C:\path\to\your\lolbas.dll
```

Use case:	Local execution of managed code to bypass AppLocker.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1218
Tags:	Execute: DLL