bohops / AccCheckConsole.txt

Last active 8 months ago

AccChecker LOLBIN [AccCheckConsole.exe]

AccCheckConsole.txt Raw

```
*Purpose
 - UI Accessibility Checker
 - Verifies UI accessibility requirements

*LOLBIN Functionality/Steps
 1) Go to "Custom Verification Routines" link in reference section and copy the sample verification C#
 2) Add proper assembly references (e.g. AccCheck.dll)
 3) Insert your C# code under a target method such as Execute()
 4) Compile to a .NET managed library (DLL)
 5) Invoke the code
   a) There are several ways to do this. Easiest is to specify a program window name (e.g. you are goin
      For POC, I'd recommend just opening notepad.exe and using the default Window name - "Untitled - N
   b) Run the following command:

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

*LOLBAS Categories
 - Other MS Binary
 - Execute
 - AWL Bypass (AppLocker)

*Location(s)
 - From Windows SDK
 - C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x86\AccChecker
 - C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x64\AccChecker
 - c:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm\AccChecker
 - c:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm64\AccChecker
```

```
28    - (Other locations likely depending on SDK version and architecture)
29
30  *Testing
31    - Windows 10 Pro
32    - Windows 10 Enterprise
33    - Windows 11 Enterprise
34
35  *Detection/Prevention
36    - Quick KQL Search: process.name:"AccCheckConsole.exe" and process.command_line: *window* and process.
37    - WDAC blocks execution of unsigned DLL
38
39  *References:
40      - General: https://docs.microsoft.com/en-us/windows/win32/winauto/ui-accessibility-checker
41      - AccCheckConsole: https://docs.microsoft.com/en-us/windows/win32/winauto/the-accchecker-console
42      - Custom Verification Routines: https://docs.microsoft.com/en-us/windows/win32/winauto/custom-verific
```