

Instantly share code, notes, and snippets.



bohops / AccCheckConsole.txt

Last active 8 months ago

☆ Star 10

🔗 Fork 3

<> Code

🔄 Revisions 6

☆ Stars 10

🔗 Forks 3

Embed ▾

<script sr



Download ZIP

AccChecker LOLBIN [AccCheckConsole.exe]

<> AccCheckConsole.txt

Raw

```
1  *Purpose
2  - UI Accessibility Checker
3  - Verifies UI accessibility requirements
4
5  *LOLBIN Functionality/Steps
6  1) Go to "Custom Verification Routines" link in reference section and copy the sample verification C#
7  2) Add proper assembly references (e.g. AccCheck.dll)
8  3) Insert your C# code under a target method such as Execute()
9  4) Compile to a .NET managed library (DLL)
10 5) Invoke the code
11   a) There are several ways to do this. Easiest is to specify a program window name (e.g. you are going to
12       For POC, I'd recommend just opening notepad.exe and using the default Window name - "Untitled - Notepad")
13   b) Run the following command:
14
15   AccCheckConsole.exe -window "Untitled - Notepad" C:\path\to\your\lolbas.dll
16
17 *LOLBAS Categories
18 - Other MS Binary
19 - Execute
20 - AWL Bypass (AppLocker)
21
22 *Location(s)
23 - From Windows SDK
24 - C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x86\AccChecker
25 - C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x64\AccChecker
26 - c:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm\AccChecker
27 - 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
```

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.