.. /VisualUiaVerifyNative.exe

AWL bypass

A Windows SDK binary for manual and automated testing of Microsoft UI Automation implementation and controls.

Paths:
c:\Program Files (x86)\Windows Kits\10\bin\<version>\arm64\UIAVerify\VisualUiaVerifyNative.exe
c:\Program Files (x86)\Windows Kits\10\bin\<version>\x64\UIAVerify\VisualUiaVerifyNative.exe
c:\Program Files (x86)\Windows Kits\10\bin\<version>\UIAVerify\VisualUiaVerifyNative.exe

Resources:
- https://bohops.com/2020/10/15/exploring-the-wdac-microsoft-recommended-block-rules-visualuiaverifynative/
- https://github.com/MicrosoftDocs/windows-itpro-docs/commit/937db704b9148e9cee7c7010cad4d00ce9c4fdad

Acknowledgements:
- Lee Christensen (@tifkin)
- Jimmy (@bohops)

Detections:
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- Sigma: https://github.com/SigmaHQ/sigma/blob/6b34764215b0e97e32cbc4c6325fc933d2695c3a/rules/windows/process_creation/proc_creation_win_lolbin_visualuiaverifynative.yml
- IOC: As a Windows SDK binary, execution on a system may be suspicious

AWL bypass

Generate Serialized gadget and save to - C:\Users\[current user]\AppData\Roaminguiverify.config before executing.

```
VisualUiaVerifyNative.exe
```

Use case:	Execute proxied payload with Microsoft signed binary to bypass WDAC policies
Privileges required:	User
Operating systems:	Windows 10 2004 (likely previous and newer versions as well)
ATT&CK® technique:	T1218