





Sign in


 LOLBAS-Project / LOLBAS Public


 Notifications


 Fork 990


 Star 7.1k


<> Code


 Issues 20

 Pull requests 20

 Actions

 Projects

 Security

 Insights

LOLBAS / yml / LOLUtilz / OSBinaries / Powershell.yml 





18 lines (17 loc) · 547 Bytes

Code

Blame

Raw







```
1  ---
2  Name: Powershell.exe
3  Description: Execute, Read ADS
4  Author: ''
5  Created: '2018-05-25'
6  Categories: []
7  Commands:
8    - Command: powershell -ep bypass - < c:\temp:ttt
9      Description: Execute the encoded PowerShell command stored in an Alternate Data Stream (ADS).
10 Full_Path:
11   - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
12   - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
13 Code_Sample: []
14 Detection: []
15 Resources:
16   - https://twitter.com/Moriarty_Meng/status/984380793383370752
17 Notes: Thanks to Moriarty - @Moriarty_Meng
```

