Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

LOLBAS-Project / **LOLBAS** Public

Notifications Fork 991 Star 7.1k

Code Issues 20 Pull requests 20 Actions Projects Security Insights

Files

4db780e

Go to file

- Archive-Old-Version
- Logo
- yml
  - LOLUtilz
    - OSBinaries
      - Explorer.yml
      - Netsh.yml
      - Nltest.yml
      - Openwith.yml
      - Powershell.yml
      - Psr.yml
      - Robocopy.yml
    - OtherBinaries
    - OtherMSBinaries
    - OtherScripts
  - OSBinaries
  - OSLibraries
  - OSScripts
  - OtherMSBinaries
- Backlog.txt
- CONTRIBUTING.md
- CategoryList.md
- README.md
- YML-Template.yml

LOLBAS / yml / LOLUtilz / OSBinaries / **Powershell.yml**

api0cradle Major changes to Web portal - Small fixes to source files to ... 94368c1 · 6 years ago **History**

Code Blame 18 lines (17 loc) · 547 Bytes Raw

```yaml
---
Name: Powershell.exe
Description: Execute, Read ADS
Author: ''
Created: '2018-05-25'
Categories: []
Commands:
  - Command: powershell -ep bypass - < c:\temp:ttt
    Description: Execute the encoded PowerShell command stored in an Alternate Data Str
Full_Path:
  - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
  - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Code_Sample: []
Detection: []
Resources:
  - https://twitter.com/Moriarty_Meng/status/984380793383370752
Notes: Thanks to Moriarty - @Moriarty_Meng
```