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

8283d8d

Go to file

- .github
- Archive-Old-Version
- Logo
- yml
  - OSBinaries
    - AppInstaller.yml
    - Aspnet_Compiler.yml
    - At.yml
    - Atbroker.yml
    - Bash.yml
    - Bitsadmin.yml
    - Certoc.yml
    - Certreq.yml
    - Certutil.yml
    - Cmd.yml
    - Cmdkey.yml
    - Cmdl32.yml
    - Cmstp.yml
    - ConfigSecurityPolicy.yml
    - Conhost.yml
    - Control.yml
    - Csc.yml
    - Cscript.yml
    - DataSvcUtil.yml
    - Desktopimgdownldr.yml
    - Dfsvc.yml
    - Diantz.yml
    - Diskshadow.yml
    - Dnscmd.yml
    - Esentutl.yml
    - Eventvwr.yml
    - Expand.yml
    - Explorer.yml
    - Extexport.yml
    - Extrac32.yml
    - Findstr.yml

LOLBAS / yml / OSBinaries / Wab.yml

History

Code Blame 28 lines (28 loc) · 992 Bytes

Raw

```yaml
---
Name: Wab.exe
Description: Windows address book manager
Author: 'Oddvar Moe'
Created: 2018-05-25
Commands:
  - Command: wab.exe
    Description: Change HKLM\Software\Microsoft\WAB\DLLPath and execute DLL of choice
    Usecase: Execute dll file. Bypass defensive counter measures
    Category: Execute
    Privileges: Administrator
    MitreID: T1218
    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Full_Path:
  - Path: C:\Program Files\Windows Mail\wab.exe
  - Path: C:\Program Files (x86)\Windows Mail\wab.exe
Code_Sample:
  - Code:
Detection:
  - Sigma: https://github.com/SigmaHQ/sigma/blob/a80c29a7c2e2e500a1a532db2a2a8bd69bd4a6
  - IOC: WAB.exe should normally never be used
Resources:
  - Link: https://twitter.com/Hexacorn/status/991447379864932352
  - Link: http://www.hexacorn.com/blog/2018/05/01/wab-exe-as-a-lolbin/
Acknowledgement:
  - Person: Adam
    Handle: '@Hexacorn'
---
```

- Finger.yml
- FltMC.yml
- Forfiles.yml
- Ftp.yml
- GfxDownloadWrapper.yml
- Gpscript.yml