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
  - OSLibraries
  - OSScripts
  - OtherMSBinaries
    - AccCheckConsole.yml
    - Adplus.yml
    - Agentexecutor.yml
    - Appvlp.yml
    - Bginfo.yml
    - Cdb.yml
    - Coregen.yml
    - Csi.yml
    - DefaultPack.yml
    - Devtoolslauncher.yml
    - Dnx.yml
    - Dotnet.yml
    - Dump64.yml
    - Dxcap.yml
    - Excel.yml
    - Fsi.yml
    - FsiAnyCpu.yml
    - Mftrace.yml
    - Msdeploy.yml
    - Msxsl.yml
    - Ntdsutil.yml
    - Powerpnt.yml
    - Procdump.yml
    - Rcsi.yml
    - Remote.yml
    - Sqldumper.yml
    - Sqlps.yml
    - Sqltoolsps.yml

LOLBAS / yml / OtherMSBinaries / **Sqltoolsps.yml**

3 people Detection Resources and Other Updates (#179) 23dd023 · 3 years ago History

Code Blame 27 lines (27 loc) · 1.19 KB Raw

```yaml
---
Name: SQLToolsPS.exe
Description: Tool included with Microsoft SQL that loads SQL Server cmdlts. A replaceme
Author: 'Oddvar Moe'
Created: 2018-05-25
Commands:
  - Command: SQLToolsPS.exe -noprofile -command Start-Process calc.exe
    Description: Run a SQL Server PowerShell mini-console without Module and ScriptBloc
    Usecase: Execute PowerShell command.
    Category: Execute
    Privileges: User
    MitreID: T1218
    OperatingSystem: Windows
Full_Path:
  - Path: C:\Program files (x86)\Microsoft SQL Server\130\Tools\Binn\sqlps.exe
Code_Sample:
  - Code:
Detection:
  - Sigma: https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258
  - Splunk: https://github.com/splunk/security_content/blob/aa9f7e0d13a61626c69367290ed
Resources:
  - Link: https://twitter.com/pabraeken/status/993298228840992768
  - Link: https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sq
Acknowledgement:
  - Person: Pierre-Alexandre Braeken
    Handle: '@pabraeken'
---
```

Squirrel.yml

Te.yml

Tracker.yml

Update.yml

VSIISExeLauncher.yml

VisualUiaVerifyNative.yml