Sign in

LOLBAS-Project / **LOLBAS** Public

Notifications · Fork 990 · Star 7.1k

Code · Issues 20 · Pull requests 20 · Actions · Projects · Security · Insights

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

27 lines (27 loc) · 1.19 KB

Code · Blame · Raw

```yaml
---
Name: SQLToolsPS.exe
Description: Tool included with Microsoft SQL that loads SQL Server cmdlts. A replacement for sqlps
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 ScriptBlock Logging.
    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/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/wir
  - Splunk: https://github.com/splunk/security_content/blob/aa9f7e0d13a61626c69367290ed1b7b71d1281f
Resources:
  - Link: https://twitter.com/pabraeken/status/993298228840992768
  - Link: https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sql-server-201
Acknowledgement:
  - Person: Pierre-Alexandre Braeken
    Handle: '@pabraeken'
```

```
---
```