.. /Sqlps.exe

Execute

Tool included with Microsoft SQL Server that loads SQL Server cmdlets. Microsoft SQL Server\100 and 110 are Powershell v2. Microsoft SQL Server\120 and 130 are Powershell version 4. Replaced by SQLToolsPS.exe in SQL Server 2016, but will be included with installation for compatability reasons.

Paths:
C:\Program files (x86)\Microsoft SQL Server\100\Tools\Binn\sqlps.exe
C:\Program files (x86)\Microsoft SQL Server\110\Tools\Binn\sqlps.exe
C:\Program files (x86)\Microsoft SQL Server\120\Tools\Binn\sqlps.exe
C:\Program files (x86)\Microsoft SQL Server\130\Tools\Binn\sqlps.exe
C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\SQLPS.exe

Resources:
- https://twitter.com/ManuelBerrueta/status/1527289261350760455
- https://twitter.com/bryon_/status/975835709587075072
- https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sql-server-2017

Acknowledgements:
- Bryon (@bryon_)
- Manny (@ManuelBerrueta)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_mssql_sqlps_susp_execution.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/image_load/image_load_dll_system_management_automation_susp_load.yml
- Elastic: https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/execution_suspicious_powershell_imgload.toml
- Splunk: https://github.com/splunk/security_content/blob/aa9f7e0d13a61626c69367290ed1b7b71d1281fd/docs/_posts/2021-10-05-suspicious_copy_on_system32.md

Execute

Run a SQL Server PowerShell mini-console without Module and ScriptBlock Logging.

```
Sqlps.exe -noprofile
```

Use case: Execute PowerShell commands without ScriptBlock logging.

Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218