

.. /Setupapi.dll

AWL bypass (INF)

Execute (INF)

Windows Setup Application Programming Interface

Paths:

c:\windows\system32\setupapi.dll

c:\windows\syswow64\setupapi.dll

Resources:

- <https://github.com/huntresslabs/evading-autoruns>
- <https://twitter.com/pabraeken/status/994742106852941825>
- https://windows10dll.nirsoft.net/setupapi_dll.html

Acknowledgements:

- Kyle Hanslovan (COM Scriptlet) ([@KyleHanslovan](#))
- Huntress Labs (COM Scriptlet) ([@HuntressLabs](#))
- Casey Smith (COM Scriptlet) ([@subTee](#))
- Nick Carr (Threat Intel) ([@ItsReallyNick](#))

Detections:

- Sigma:
https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_rundll32_setupapi_installhinfsection.yml
- Sigma:
https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml
- Splunk:
https://github.com/splunk/security_content/blob/86a5b644a44240f01274c8b74d19a435c7dae66e/detections/endpoint/detect_rundll32_application_control_bypass__setupapi.yml

AWL bypass

Execute the specified (local or remote) .wsh/.sct script with scrobj.dll in the .inf file by calling an information file directive (section name specified).

```
rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall 128 C:\Tools\shady.inf
```

Use case: Run local or remote script(let) code through INF file specification.

Privileges required: User

Operating systems: Windows 10, Windows 11

ATT&CK® technique: T1218.011

Tags:

Input: INF

Execute

Launch an executable file via the InstallHinfSection function and .inf file section directive.

```
rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall 128 C:\Tools\calc_exe.inf
```

Use case: Load an executable payload.

Privileges required: User

Operating systems: Windows

ATT&CK® technique: T1218.011

Tags: Input: INF