# .. /Regedit.exe

Alternate data streams

Used by Windows to manipulate registry

**Paths:**
C:\Windows\regedit.exe

**Resources:**
- https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

**Acknowledgements:**
- Oddvar Moe (@oddvarmoe)

**Detections:**
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_regedit_import_keys_ads.yml
- IOC: regedit.exe reading and writing to alternate data stream
- IOC: regedit.exe should normally not be executed by end-users

## Alternate data streams

. Export the target Registry key to the specified .REG file.

```
regedit /E c:\ads\file.txt:regfile.reg HKEY_CURRENT_USER\MyCustomRegKey
```

**Use case:** Hide registry data in 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

. Import the target .REG file into the Registry.

```
regedit C:\ads\file.txt:regfile.reg
```

**Use case:** Import hidden registry data 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