.. /Regini.exe

Alternate data streams

Used to manipulate the registry

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

Resources:

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

Acknowledgements:

- Eli Salem (@elisalem9)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_regini_ads.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_regini_execution.yml
- IOC: regini.exe reading from ADS

Alternate data streams

Write registry keys from data inside the Alternate data stream.

```
regini.exe newfile.txt:hidden.ini
```

Use case:	Write to registry
Privileges required:	User
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1564.004