.. /Psr.exe ☆ Star

Reconnaissance

Windows Problem Steps Recorder, used to record screen and clicks.

Paths:
c:\windows\system32\psr.exe
c:\windows\syswow64\psr.exe

Resources:

- https://social.technet.microsoft.com/wiki/contents/articles/51722.windows-problem-steps-recorder-psr-quick-and-easy-documenting-of-your-steps-and-procedures.aspx

Acknowledgements:

- Leon Rodenko (@L3m0nada)

Detections:

- Sigma: proc_creation_win_psr_capture_screenshots.yml
- IOC: psr.exe spawned
- IOC: suspicious activity when running with "/gui 0" flag

Reconnaissance

Record a user screen without creating a GUI. You should use "psr.exe /stop" to stop recording and create output file.

```
psr.exe /start /output D:\test.zip /sc 1 /gui 0
```

Use case:	Can be used to take screenshots of the user environment
Privileges required:	User
Operating systems:	since Windows 7 (client) / Windows 2008 R2
ATT&CK® technique:	**T1113**: Screen Capture