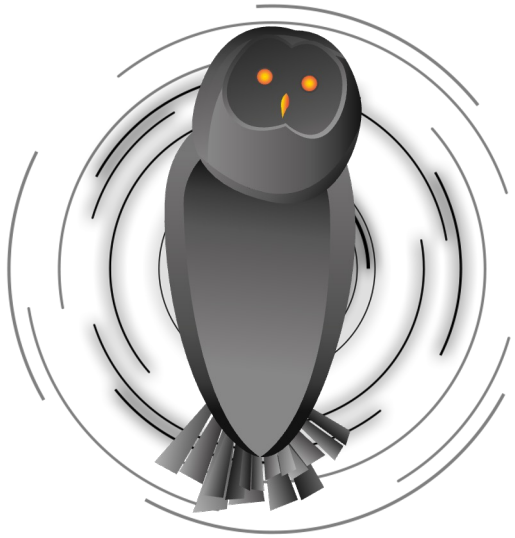


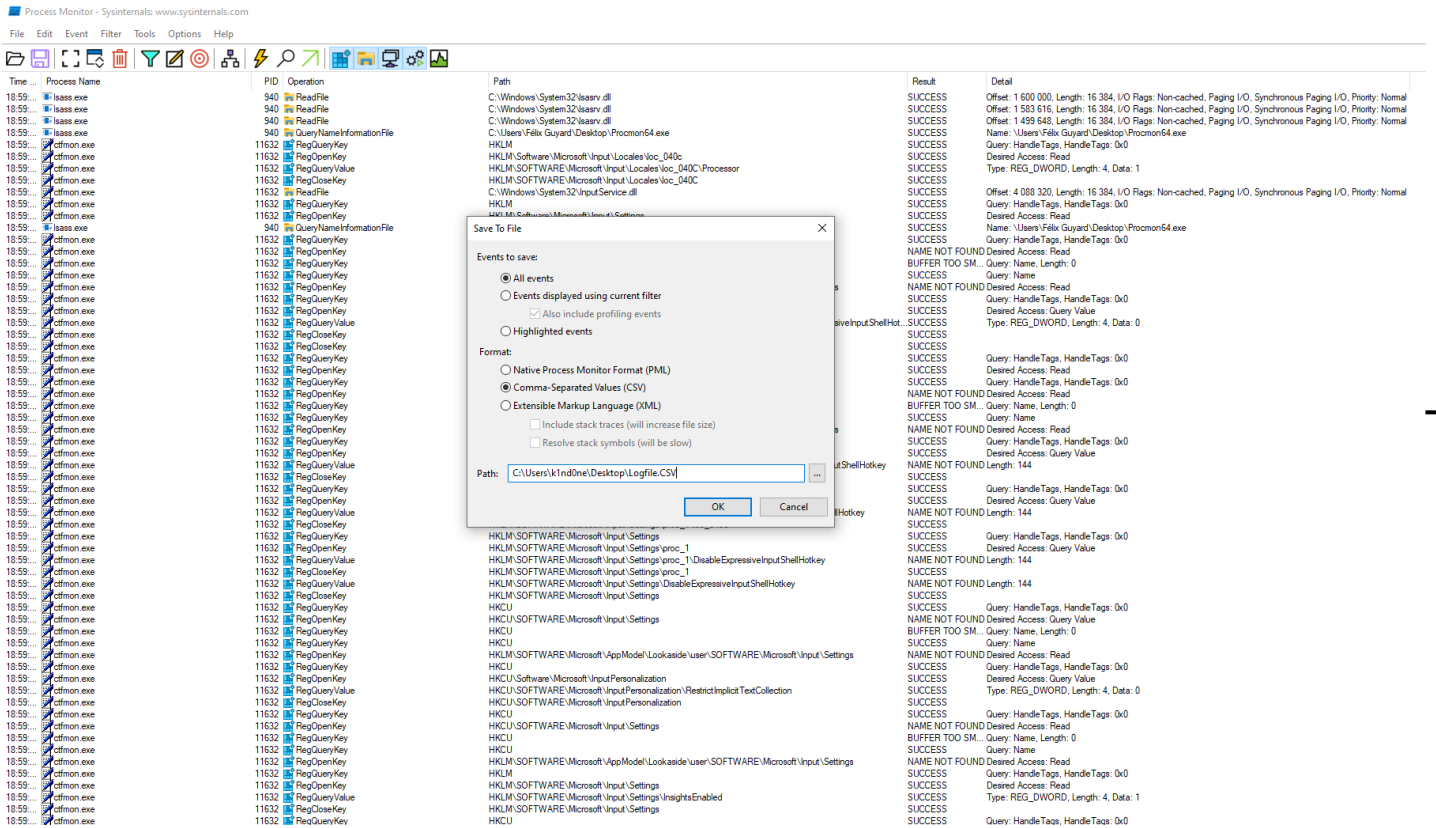
VISION-ProcMon

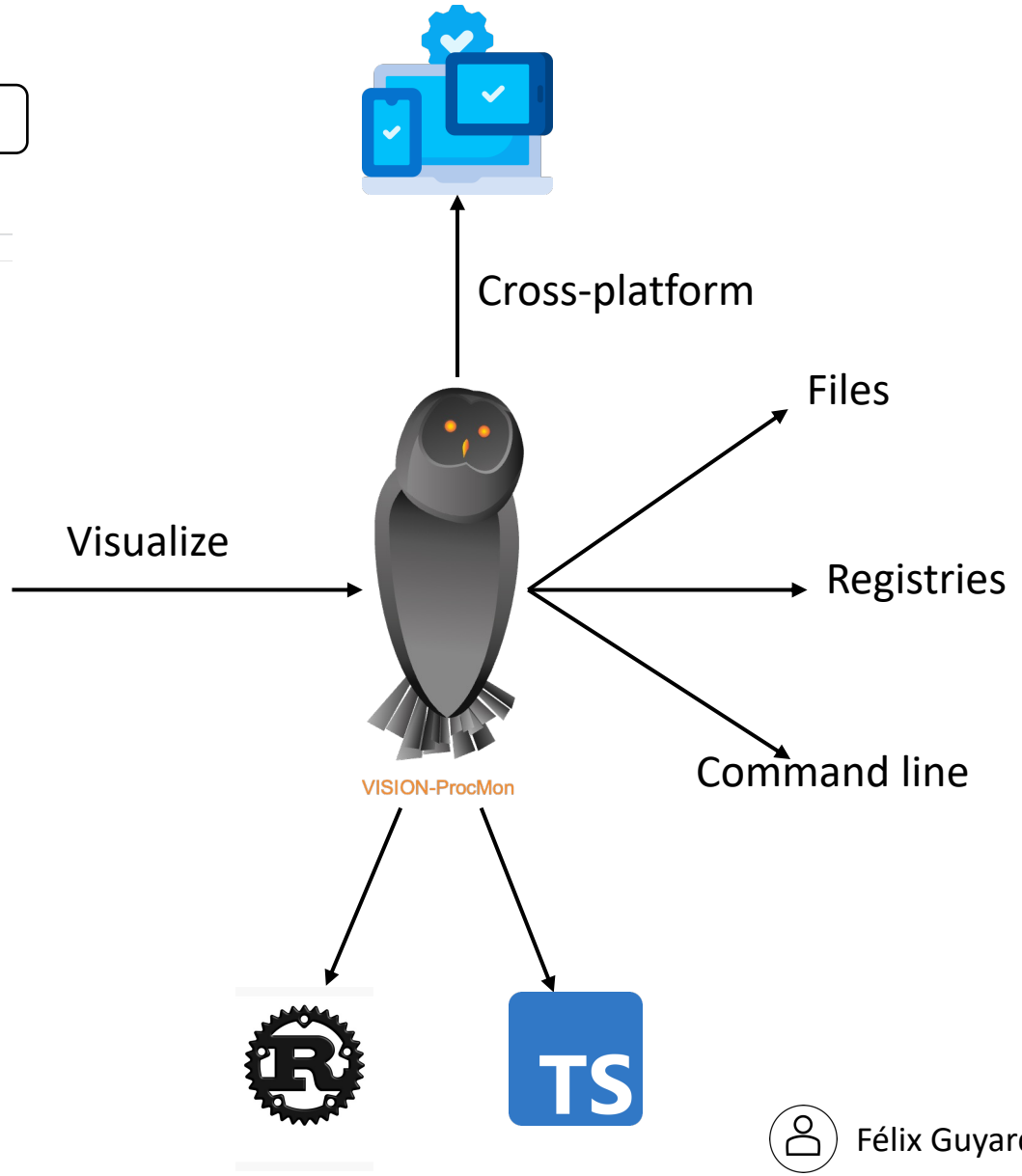
Visualization tool dedicated to malware analysts

Félix Guyard

0 – Intro

Performing a behavioral analysis using procmon is a step into identifying more TTPs & IOCs





1 – Demo

2 – Thanks

Twitter @k1nd0ne
Contact me : felix.guyard@forensicxlab.com

https://github.com/forensicxlab/VISION-ProcMon
https://github.com/k1nd0ne/