

VISION-ProcMon

Visualization tool dedicated to malware analysts

0 – Intro



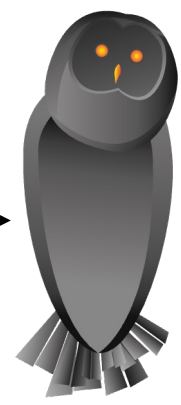
Performing a behavioral analysis using procmon is a step into identifying more TTPs & IOCs

The screenshot shows the Process Monitor interface with a list of events and a 'Save To File' dialog box. The dialog box has the following options:

- Events to save:
 - All events
 - Events displayed using current filter
 - Highlighted events
- Format:
 - Native Process Monitor Format (PML)
 - Comma-Separated Values (CSV)
 - Extensible Markup Language (XML)
- Path: C:\Users\k\OneDrive\Desktop\Logfile.CSV



Cross-platform



Visualize

Files

Registries

Command line

VISION-ProcMon





2 – Thanks



Twitter @k1nd0ne

Contact me : felix.guyard@forensicxlab.com

<https://github.com/forensicxlab/VISION-ProcMon>

<https://github.com/k1nd0ne/>