Visual Mining of Operating System Process Information

Adam Fuchs(CS)

Chang-Han Jong(ECE)
InfoViz Supports Anomaly Detection

Ex. Object files contain certain signature

Ex. Modeling memory usage by HMM

InfoVis: using human for intrusion detection
Windows Task Manager

- CPU Time, Mem Usage, IO Reads, IO Writes
Scenario

Show
- Show process resource in hierarchy
- Ex. Load|CPU|IO Writes|IO Reads|Network Activity

Identify
- Find the process that use much resource
- Ignore normal usage. Ex. Starting up process

Reference
- Check web for malware description

History
- Watch this program’s previous behavior

Kill
- Kill related processes