Workflow of a security analyst

Using Viper as a management console for malware analysis

CIRCL
Computer Incident
Response Center
Luxembourg

TLP:WHITE

info@circl.lu

March 22, 2016

Context

- Task: analyze a malware
- Problem: can be an Hash, in a mail, a sample, a MISP event...
- Tools: IDA, radare2,
- Services: Passive DNS, Passive SSL, VirusTotal, Cuckoo, MISP
- Extra problem: Information sharing

PyMISP

- Easy interface to query MISP instances through the REST API
- Comes with standalone script to do a some specific queries
- Follows very closely the evolution of the MISP code
- Supports al the functionalities of MISP
- Workflow-oriented: many helpers to make integration easyer

Viper

- Solid CLI
- Django interface is available (I've been told)
- Plenty of modules
- Locale storage of your own zoo

PyMISP & Viper

- Full featured CLI for MISP
- Search / Cross check with VT
- Create / Update / Show / Publish Event
- Download / Upload Samples
- Mass export / upload / download
- Get Yara rules

Viper & VT

- Searches for hashes/ips/domains/URLs from the current MISP event, or download the samples
- Download samples from current MISP event
- Download all samples from all the MISP events of the current session

Other modules

- Fully featured CLI for Passive SSL
- Fully featured CLI for Passive DNS
- Can launch Radare2 or IDA
- ... And let's look at it in the demo.

Conclusion

- https://github.com/CIRCL/PyMISP
- https://github.com/viper-framework/viper
- https://github.com/MISP/MISP
- Any request / issues should be opened on Github to keep track