Malware Forensics - Behavioral Analysis and Detection with Open Source EDR

Degree programme : MAS Digital Forensics & Cyber Investigation

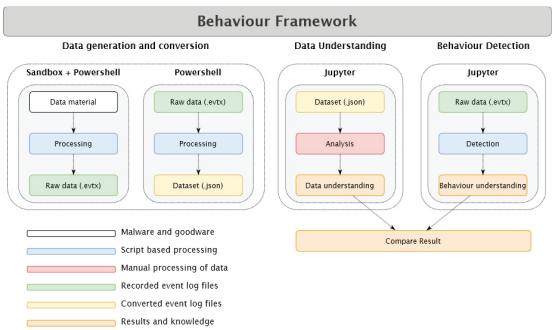
The constantly growing amount of data and the threat to IT security require new approaches to data detection and analysis. The focus of this thesis is set on using open-source endpoint telemetry and detection. For this purpose, Microsoft Sysmon and Sigma are analyzed. Analysis helpers are developed to extend the use of the existing solution. The usage of this framework in forensic analysis as well as future applications will be discussed.

Initial situation and objectives

Modern threat hunting is confronted with quickly growing data volumes. Context detection is becoming more complicated as malware behavior is becoming more and more intelligent. This increases the difficulty of detection and identification. The behavioral differences between legit and malicious software are also narrowing causing these new threats to remain undetected. The goal of this work is to investigate how to mitigate this situation using open-source detection and telemetry. Data acquisition, required helper tools, data quality as well as their combined effects in forensic investigations are discussed here. A detection framework is set up that will help to answer these questions. The aim of this work is to investigate the suitability of open-source detection and sensors for telemetry and which extensions would be required. It should be shown whether a process behavior of known and unknown software is recognizable and detectable.

Limitations

Optimization possibilities of Sigma Rules are mentioned in the concept but not implemented. The generated code elements only serve as a demonstration for the proof of concept and do not comply with common programming standards. Well known forensic tools and environments were deliberately omitted to focus on the potential of Microsoft Sysmon and Sigma rules.



Framework for behaviour understanding

Methods

Data material is generated in a laboratory environment built on the model of a detonation sandbox. The obtained data is collected centrally and datasets are created. The analysis of the obtained data is performed with Jupyter and Python. Detection of the potentially present malware is realized with Sigma. Finally, optimization options are identified.

Matthias Turczyn

Results and further enhancements

Existing open-source technologies have been enhanced and integrated in a framework that increases the speed and quality of malware detection. The data material is analyzed with the help of this framework and available threat intelligence reports. The quality of the results has validated the usage of Microsoft Sysmon as a data source and sensor. With another module from this framework, applied to the collected data, Sigma detection rules were tested to evaluate the detection efficiency. With the knowledge gained from the analyses and detection results, further optimizations were made. Application possibilities of the connection to Elasticsearch and handling of „cold“ or „old“ data were also verified.

Conclusions

This work shows which options and improvements are possible when using open-source sensors and detectors. The most prominent results of this analysis are:

- Microsoft Sysmon is well suited as a data source.
- The balanced between data quantity and quality must be permanently reevaluated to maintain the quality of the result.
- Microsoft Sysmon does not replace existing SIEM systems or other analytical frameworks.
- The enhanced Microsoft Sysmon/Sigma framework offers an extension of current threat hunting solutions without replacing them.