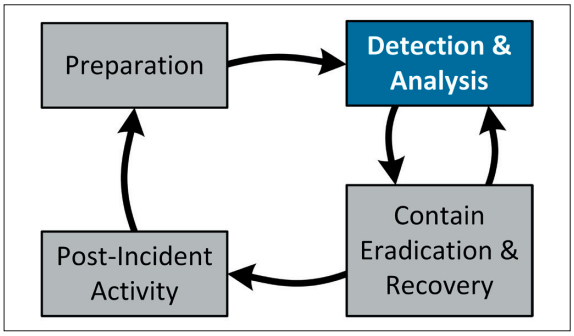
Roman Ehrbar

Oliver Gerard Nietlispach

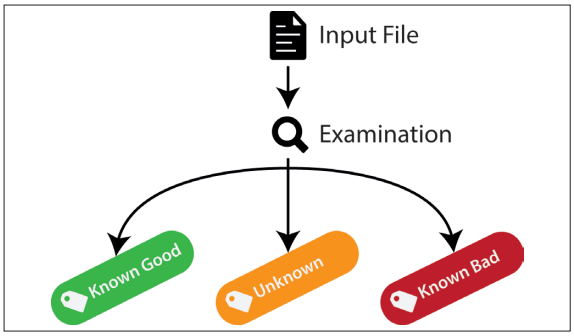
Graduate Candidates	Roman Ehrbar, Oliver Gerard Nietlispach
Examiner	Cyrill Brunschwiler
Co-Examiner	Dr. Benjamin Fehrensen, UBS
Subject Area	Sicherheit

Malware Hunting

Maloney – a Forensic Triage Toolkit



Incident Response Life Cycle as defined by the National Institute of Standards and Technology (NIST)



Categorization of a file as performed by Maloney

Introduction: The analysis of potentially compromised workstations and servers has become daily routine for a security analyst. To help during the detection and analysis process, a triage toolkit is used which uses various methods to categorize data of a potentially comprised system. A good triage toolkit removes as much known data from the list, which leaves less work for the analyst. An approach to reduce the data set is using white- and blacklists of known software components. In a previous term project, a prototype called Maloney had been developed which sought to improve on existing solutions in matters of automation and recoverability. In this bachelor thesis, the aim is to further analyze requirements and to extend Maloney.

Approach/Technologies: The bachelor thesis was separated into multiple week-long iterations for which the goals and results were individually defined. During these iterations, analyses, approaches and solutions for individual requirements were formulated and implemented. Maloney is built on Java, Elasticsearch and The Sleuth Kit (TSK) and is an event-driven framework. An examination is broken down into smaller processes, called Jobs. These are run in sequence and generate events which then get passed on to further subscribed Jobs. The application uses Elasticsearch to speed up lookups of aggregated meta-data. TSK extracts files and meta-data from disk images. Additional features and technologies were added, such as MapDB for resilience and Jsign for the verification of signed software.

Result: Many new features have been added to Maloney during the bachelor thesis. Currently, the examination process itself supports hash and signature comparisons only. But further examination methods can be seamlessly added through the plug-in mechanism. These Jobs are now run in multiple threads. Tolerance to faults has been added by the inclusion of a recoverable, persistent storage for events. Even after an unexpected crash, the application can proceed the examination. After all data has been extracted and examined, a report can be generated with a categorization based on customizable rules. Alternatively, the data can be viewed in Elasticsearch or queried through a Command Line Interface (CLI).