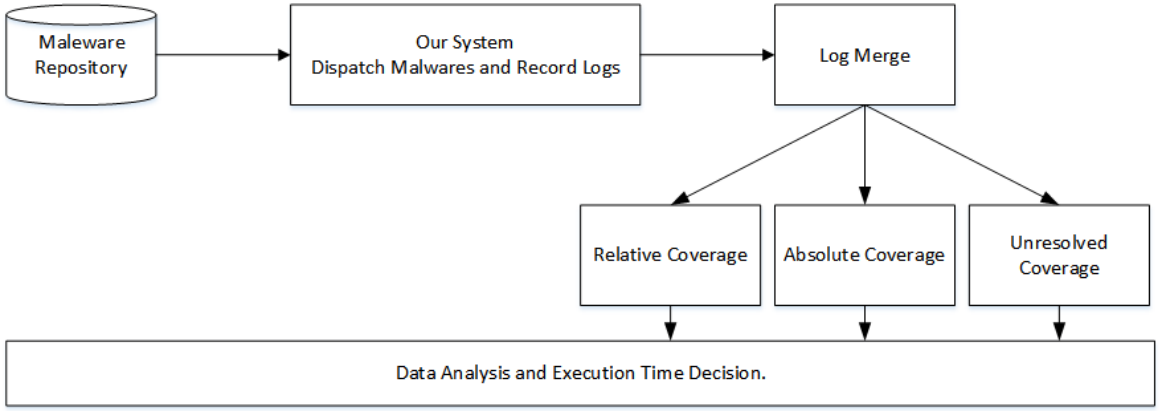
The Rhythm of Execution: Unveiling the Impact of Sandbox Execution Time on Cyber Threat Intelligence data

Xuguo WANG, Diming ZHANG, Chenglin LI, Xuan JIANG

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50245-y

Problems & Ideas

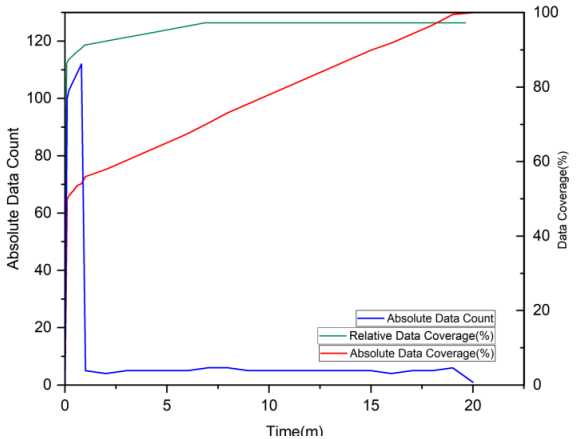
- Problems of conventional sandbox-based CTI data collection approaches:
  - Existing sandbox systems set execution time thresholds arbitrarily, without considering the dynamic nature of malware behavior.
  - Premature termination may cause loss of critical threat intelligence data; overlong execution leads to unnecessary resource waste.
  - There is a lack of empirical modeling on how execution time impacts intelligence data completeness and fidelity.
- Ideas:
  - Propose a quantitative execution time optimization framework based on Extreme Value Theory (EVT), analyzing the temporal evolution of intelligence data.
  - Leverage system call sequences, code execution, and data entry access patterns (mapped to MITRE ATT&CK TTPs) to model and predict intelligence acquisition trends.



Malware samples are dispatched from the repository and their execution behaviors are recorded. Logs from different sources are merged into a unified timeline to ensure data consistency.Three behavior coverage metrics—Relative, Absolute, and Unresolved Coverage—are then computed.Finally, data analysis combined with Extreme Value Theory (EVT) modeling is performed to determine the optimal sandbox execution time, balancing intelligence completeness and efficiency.

Main Contributions

- Contributions:
  - Proposed a quantitative execution time optimization framework for sandbox-based cyber threat intelligence (CTI) data collection, using Extreme Value Theory (EVT) to model intelligence data growth trends;
  - Designed and implemented a comprehensive data collection system that integrates traditional sandbox, PANDA, and KleAm to achieve fine-grained coverage of system calls, code execution, and data access behaviors;
  - Demonstrated that over 90% of intelligence data is extracted within the first 3 minutes, and the probability of observing new threat intelligence rapidly decreases with time, providing practical guidance for setting optimal sandbox execution time.



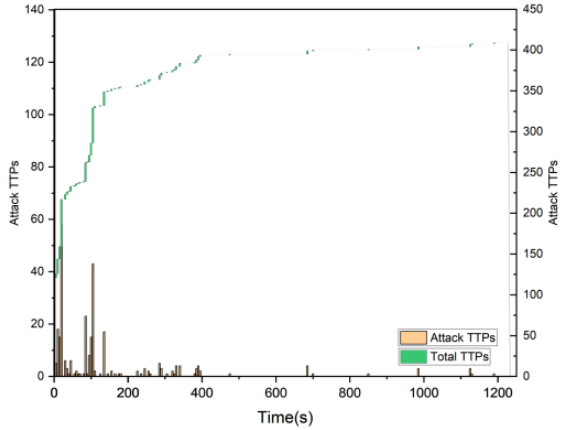


Table 6 Probability of Observing New Intelligence Data Beyond a Given Execution Time.

Execution Time (s)	180	240	300	360	600
$P(T > t)$	0.092	0.081	0.074	0.069	0.056

The probability of acquiring new intelligence data decreases over time, dropping from 0.092 at 180 seconds to 0.056 at 600 seconds, indicating diminishing returns with extended execution.