Automatisierte Anomalie-Detektion in der Memory-Forensik

Fachgebiet: Informatik - IT Security
Betreuer: Dr. Endre Bangerter
Experte: Dr. Federico Flueckiger (Informatik und Telekommunikation EFD)

Die Bedrohungen durch Malware und gezielte Hacking-Angriffe nehmen weltweit stetig zu. Gleichzeitig wird es aufgrund der steigenden Komplexität der Angriffe immer schwieriger, diese zu entdecken. Eine Schlüsseltechnik für die Erkennung von Angriffen und die Analyse von Malware ist die Memory-Forensik. Basierend auf dieser Technik wurde eine Applikation entwickelt, welche eine automatisierte Detektion der von Malware verursachten Anomalien ermöglicht.

Die Memory-Forensik beschäftigt sich mit der Untersuchung sog. Memory-Dumps, also Momentanaufnahmen des Arbeitsspeichers. Während Malware ihre Spuren und Dateien auf der Festplatte eines Systems erfolgreich verstecken kann, ist dies im Arbeitsspeicher kaum möglich.

Das quelloffene Memory-Forensik-Framework Volatility bietet umfangreiche Werkzeuge und Plugins an, um verschiedenste Informationen aus Memory-Dumps zu lesen. Mit diesen Informationen sollen die Spuren von Malware ausfindig gemacht werden. Die Interpretation der Informationen bedingt jedoch tief reichende System- und Malware-Kenntnisse, da die verursachten Anomalien oft sehr subtil sind. Solche Analysen sind somit nur wenigen Spezialisten zugänglich und erfordern gleichzeitig viel Zeit.

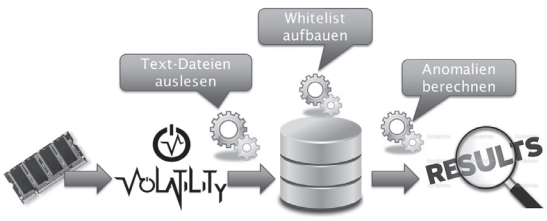
Es existieren bereits Lösungen zur automatischen Memory-Dump-Analyse und Anomalie-Detektion. Diese stellen jedoch sog. Black-Box-Lösungen dar: für den Anwender sind nur die Eingabe und das berechnete Ergebnis ersichtlich, wie die Anomalien detektiert wurden ist nicht nachvollziehbar, ebenso wenig kann die Vollständigkeit der Resultate eingeschätzt werden.

Die im Rahmen dieser Thesis entwickelte Applikation ermöglicht eine weitgehende Automatisierung der Anomalie-Detektion in Memory-Dumps von Windows 7Systemen. Dank dem gewählten White-Box-Ansatz sind die berechneten Resultate vollständig nachvollziehbar. Basierend auf den von Volatility ausgegebenen Daten wird eine Whitelist aufgebaut, welche die charakteristischen System-Informationen unversehrter Memory-Dumps enthält. Aus dem Vergleich derselben charakteristischen System-Informationen potentiell infizierter Memory-Dumps mit der zuvor aufgebauten Whitelist resultieren die durch Malware verursachten Anomalien. Als Ergänzung werden auch die aus den Memory-Dumps extrahierten Programmdateien untersucht, um zusätzliche Anomalien zu detektieren. Die Ergebnisse können für weitere Untersuchungen übersichtlich in einem Web-Frontend dargestellt oder als CSV-Datei exportiert werden.

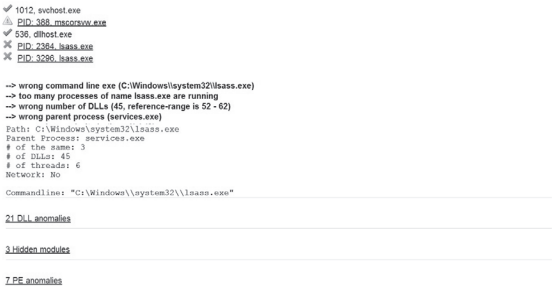
Systematische Praxis-Tests zeigten, dass unser Ansatz sehr gute Detektions-Ergebnisse bei einer gleichzeitig geringen False-Positive-Rate liefert; sie kommen nahe an die Qualität der von Experten durchgeführten manuellen Malware-Analysen heran. Das Ziel, eine offene und nachvollziehbare Applikation für die automatisierte Anomalie-Detektion zu realisieren, haben wir somit erreicht.

Ramona Cioccarelli

Benjamin Urech



Analyse-Prozess



Web-Frontend