Automatisierte Analyse von logischen Angriffen auf Selbstbedienungssystem

Studiengang: MAS Digital Forensics & Cyber Investigation

In dieser Arbeit wurde ein Modul für die Forensik-Software Autopsy entwickelt, das die Analyse gewisser logischer Angriffe auf Selbstbedienungssysteme automatisiert. Dabei werden verschiedene Artefakte vom Betriebssystem und der Geräte-Software anhand ausgearbeiteter Regeln analysiert, bewertet und auf verschiedene Arten grafisch dargestellt.

Ausgangslage

Selbstbedienungssysteme werden regelmässig zum Ziel krimineller Aktivitäten. Dabei kommt eine Vielzahl von Angriffsmethoden zum Einsatz. Von physischen Attacken wie Vandalismus, Diebstahl oder Sprengungen über Betrugsdelikte, bei denen ein Gerät gezielt manipuliert wird, um zum Beispiel Kundendaten zu stehlen. Eine weitere Art, ein Gerät anzugreifen, sind sogenannte logische Angriffe. Dabei werden Schwachstellen in der Software oder dem Netzwerk ausgenutzt, um die Kontrolle über ein Gerät zu übernehmen und etwa Malware darauf zu installieren. Glücklicherweise hinterlassen solche Angriffe meistens diverse digitale Spuren. Aktuell müssen Ermittlerinnen und Ermittler diese Spuren von Hand oder mit einer Kombination aus unterschiedlichen Tools analysieren, was sehr zeitaufwändig ist. Ausserdem finden (fast) identische Angriffe oft mehrfach statt, was zu repetitivem Aufwand führt.

Ziel

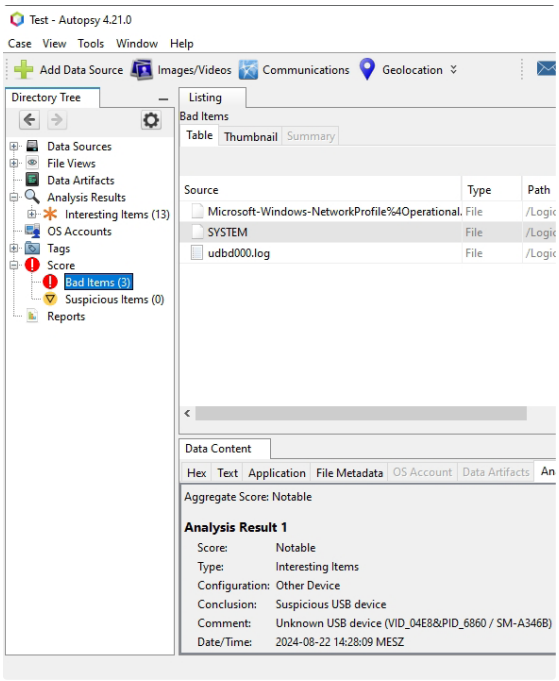
Die Ermittlerinnen und Ermittler sollen mit Software unterstützt werden, um repetitive und manuelle Arbeiten zu automatisieren und so Ressourcen für kompliziertere und zeitkritischere Fälle freizuhalten. Das Tool soll eine schnelle Einschätzung über den Erfolg eines Angriffs bieten und es auch Mitarbeitenden mit weniger Wissen in der digitalen Forensik ermöglichen, Untersuchungen zumindest teilweise zu übernehmen. Ebenfalls wichtig ist, dass das Modul konfigurierbar ist, um auch Angriffe untersuchen zu können, die nicht genauso ablaufen wie die für diese Arbeit simulierten Test-Attacken.

Vorgehen

Basierend auf früheren Erfahrungen und gezielter Simulation mehrerer logischer Angriffe auf Testgeräten wurden Artefakte von Betriebssystem und Geräte-Software identifiziert, die Hinweise auf potenzielle Angriffe liefern und automatisiert analysiert werden können. Dabei wurden Regeln erarbeitet, unter welchen Bedingungen und in welcher Kombination solche Artefakte besonders verdächtig sind. Dieses Wissen wurde als Zusatzmodul für die Forensik-Software Autopsy implementiert.

Ergebnisse

Das Modul identifiziert alle relevanten Artefakte und erkennt anhand definierter Regeln alle Test-Angriffe und einen ausgewählten echten Angriff. Alle Resultate der Analysen werden ins User Interface von Autopsy integriert und können in einer Timeline oder als Report dargestellt werden. Ausserdem erhält der Ermittler oder die Ermittlerin eine automatisierte Einschätzung, ob ein Angriff stattgefunden hat und erfolgreich war. Die Analyse dauert im Normalfall nur wenige Minuten, was im Gegensatz zu einigen Stunden manuellem Aufwand viel Zeit einspart.



Analyse-Resultate in Autopsy

Benjamin Truninger