Automatische Whitelist Generation und Studie deren Qualität

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Dr. Endre Bangerter, Beni Urech
Experte: Dr. Joachim Wolfgang Kaltz

Arbeitsspeicher-Forensik spielt beim Entdecken und Analysieren von Malware eine tragende Rolle. Hierfür sind nicht nur ausgiebige Systemkenntnisse, sondern auch viel versionsabhängiges Detail-Wissen nötig. Dieses sollte nicht auswendig gelernt, sondern von technischen Mitteln bereitgestellt werden. Vortessence stellt hierfür Whitelists zur Verfügung. Das Ziel dieser Arbeit ist nun die automatisierte Erstellung von Whitelists.

Situation

Die Arbeitsspeicher-Forensik spielt in der Entdeckung und Analyse von Malware eine zentrale Rolle, weil jedes Programm (Malware oder legitime Applikation) im Arbeitsspeicher vorhanden sein muss, um ausgeführt zu werden. Da jedoch eine Analyse tiefgehende Kenntnisse voraussetzt entwickelt das SEL (Security Engineering Lab der BFH Biel) das Speicherforensik Framework Vortessence. Dieses unterstützt die Forensik Expertin, den Forensik Experten möglichst weit durch Automation. Die bestehende Lösung benutzt ein weiteres Framework namens Rekall zur Erfassung und ersten Aufbereitung der Rohdaten und Vortessence für die übergeordnete Steuerung und weiteren Verarbeitung. Um Detail-Wissen betreffend des Normalzustandes eines Systems festzuhalten wird eine Whitelist eingesetzt. Deren Einträge, auch Artefakte genannt, beschreiben beispielsweise die laufenden Prozesse, geladene DLL's und laufende Dienste eines nicht infizierten Systems. Damit lässt sich später ein zu analysierendes System mit dem «Normalzustand» vergleichen. Die normalerweise aufwendige manuelle Erstellung einer solchen Whitelist soll nun automatisiert werden.

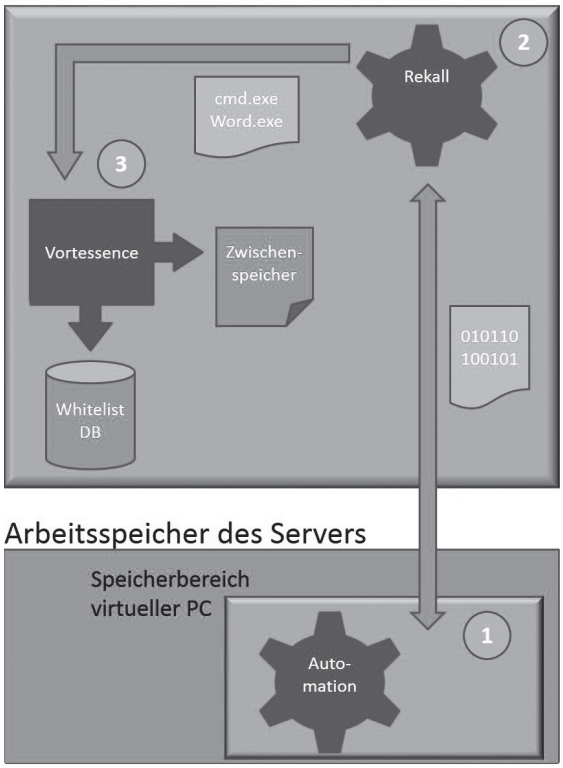
Glenn Ryser

Das System

Der bisherige Ansatz einzelne Speicherabbilder zu analysieren wird auf Memory Introspection umgestellt. Das heisst, das zu beobachtende System wird als virtuelles Gerät auf dem Server laufen gelassen, was erlaubt, direkt auf dessen Arbeitsspeicher zuzugreifen. Damit überhaupt etwas Beobachtbares vorhanden ist, wird auf dem virtuellen Gerät ein Anwender simuliert. Dies geschieht durch eine Automation, welche diverse Applikationen wie Word oder Excel ausführt und deren Dokumente manipuliert. Währenddessen kann mittels Recall der Arbeitsspeicher kontinuierlich nach Artefakten durchsucht werden. Die daraus entstandenen Rohdaten werden aufbereitet und an Vortessence übergeben. Dieses vergleicht mit einem Zwischenspeicher, ob die individuellen Artefakte bereits bekannt sind und fügt sie wenn nötig der Whitelist hinzu.

Resultate

Die Studie zur Qualität der neuen Whitelist stellt nachfolgendes fest:
Es dauert ungefähr zwei Stunden, bis die Artefakte des Systems und des Anwenders erfasst sind. Für den Einsatz in einer realen Umgebung wäre die Automation allerdings auszubauen. Weiter lässt sich eine Whitelist auf andere, ähnlich installierte Systeme anwenden. Ausserdem hat ein Test mit echter Malware ergeben, dass eine gewisse Relevanz der automatisch generierten Whitelist-Einträge gegeben ist, diese aber noch erweitert werden kann.



1. Automation in der VM, 2. Erfassung der Artefakte mit Rekall, 3. Generation der Whitelist durch Vortessence