CAPE Sandbox Evaluation

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer: Prof. Dr. Endre Bangerter
Experte: Dr. Igor Metz (Glue Software Engineering AG)

Malware ist eine immer grösser werdende Gefahr für Unternehmen wie auch Privatpersonen. Verteidigung gegen Malware ist daher eine Notwendigkeit, um sich gegen finanzielle Schäden und Verletzung der Privatsphäre zu verteidigen. Da sich Malware stetig weiterentwickelt und die Zahl stetig zunimmt, ist eine automatisierte Bekämpfung notwendig. Malware Sandboxen sind ein möglicher Ansatz dazu.

Bedrohung durch Malware

Im Jahre 2019 wurden jeden Tag 350'000 neue Malware entdeckt. Solche Zahlen sind beindruckend und beunruhigend zugleich. Malware ist eine riesige Bedrohung für Unternehmen und die gesamte Gesellschaft. Um uns gegen diesen Risiken zu verteidigen, ist es wichtig, sich dagegen schützen zu können. Wegen dieser grossen Zahl im Umlauf befindlicher Schadsoftware ist es entscheidend, eine automatisierte Lösung zu haben, welche Sicherheitsexperten in ihrer täglichen Arbeit unterstützt.

CAPE

Die Open-Source Sandbox CAPE ermöglicht es, verdächtige Schadsoftware in einer isolierten Umgebung laufen zu lassen und ihr Verhalten zu analysieren. Dies ermöglicht es, Malware sicher zu detektieren und ihre Funktionsweise besser zu verstehen. Es wird eine dynamische Analyse durchgeführt, dh. es werden unter anderem die API-Calls & auch die Netzwerk-Kommunikation aufgezeichnet, welche vom gestarteten Programm aufgerufen werden. Auch die Dateizugriffe werden dokumentiert und aus den gesammelten Daten ein Bericht erstellt. Malware Sandboxen werden in der Praxis routinemässig von Sicherheitsteams und Analysten eingesetzt.

Ziele

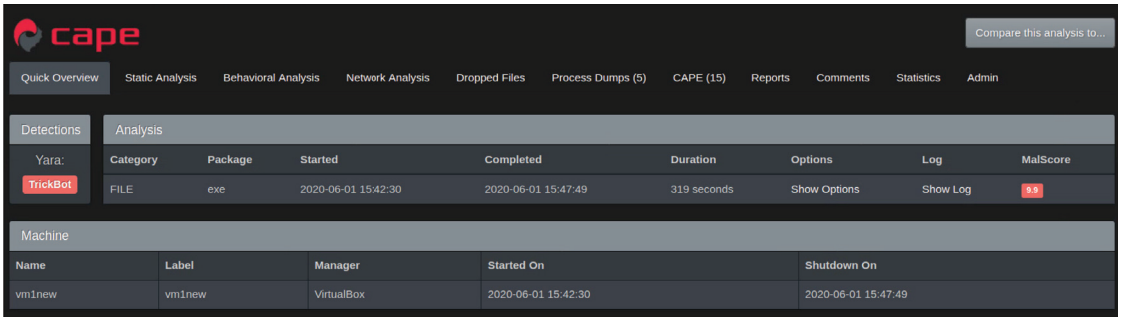
Die Evaluation der CAPE Sandbox soll auf der Grundlage von mehr als 1000 Malware Samples erfolgen. Es sollen unter anderem die Detektierbarkeit von Malware Familien, Code Injection und Memory Allocation analysiert werden. Die verschiedenen Code Injection Techniken sollten zudem studiert und dokumentiert werden. Es soll nachvollzogen werden können, welche Prozesse von einer Malware gestartet, welche Speicherbereiche von ihr alloziert werden und welche davon schädlichen Code enthalten.

Resultate

Während der Arbeit wurden mehr als 1200 Malware Samples aus 12 unterschiedlichen Malware-Familien analysiert. Die Ergebnisse zeigen, dass die Detektion von Malware relativ gut funktioniert. CAPE erkennt gefährliche Code-Ausführungen zuverlässig und die Klassifikation der Malware Familien funktioniert auch relativ gut. Das Tracking von Code Injections ist noch ausbaufähig, da noch relativ wenige Techniken abgedeckt sind und es fehlen noch einige fortgeschrittenere Daten, welche eine genauere Untersuchung von Malware ermöglichen. Da die Software allerdings aktiv weiterentwickelt wird, sehen wir diese als ernsthafte Alternative zu kommerziellen Produkten in der Zukunft.

Alessandro Allio

Martin Gräni



CAPE Web Interface