h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Hochschule Darmstadt

– Fachbereich Informatik –

Dynamische Analyse von Linux-Malware

Abschlussarbeit zur Erlangung des akademischen Grades
Bachelor of Science (B.Sc.)

vorgelegt von

Nils Rogmann
Matrikel-Nr. 725915

Referent: Prof. Dr. Marian Margraf
Korreferent: Prof. Dr. Michael Braun

Ausgabedatum: 12. Dezember 2014
Abgabedatum: 13. März 2015

Abstrakt

Sicherheitsvorfälle können im Unternehmenskontext trotz vielseitiger Schutzmaßnahmen und dem Einsatz aktueller IT-Sicherheitsinfrastrukturen niemals vollständig ausgeschlossen werden. Wird während der Bearbeitung eines Sicherheitsvorfalls, beispielsweise durch ein Incident Response-Team, potentielle Malware auf einem System entdeckt, muss diese zur Regulierung von Schäden und weiteren Infektionen sowie zum generellen Schutz von Unternehmensdaten umgehend analysiert werden. Hierbei erfolgt grundsätzlich eine Unterscheidung zwischen der statischen Analyse zur Untersuchung des zu Grunde liegenden Codes eines Schadprogramms und der dynamischen Analyse, also der kontrollierten Ausführung und dedizierten Beobachtung einer Malware.

Die Malware-Analyse soll die Eindämmung eines Sicherheitsvorfalls unterstützen sowie eine vollständige Säuberung infizierter Systeme innerhalb der Infrastruktur eines Unternehmens ermöglichen. Während zur sicheren und automatisierten Analyse von Windows-Malware bereits etablierte kommerzielle sowie nicht-kommerzielle Lösungen existieren, muss die Untersuchung von Linux-Malware bisher unter einem großen Zeitaufwand manuell durchgeführt werden.

Zielsetzung der Bachelorarbeit ist es daher, einen Prototyp zur sichereren und automatisierten Analyse von potentieller Linux-Malware zu entwickeln, der zukünftig beispielsweise im Zuge eines Incident Response-Einsatzes verwendet werden kann. Hierzu soll ein bereits zur statischen Analyse realisierter und auf der Cuckoo Sandbox basierender Prototyp, der während des vorangegangenen Praxisprojekts entwickelt wurde, um Funktionen und Techniken zur dynamischen Analyse von Linux-Malware erweitert werden.

Als Ergebnis der Bachelorarbeit wird ein Prototyp zur statischen und dynamischen Analyse von Linux-Malware zur Verfügung gestellt. Hierzu erfolgte während der Ausarbeitung die Entwicklung verschiedener Techniken zur Erfassung von Prozess-, Dateisystem- und Netzwerkaktivitäten eines zu Grunde liegenden Schadprogramms. Die Techniken wurden als Module zur dynamischen Analyse von Linux-Malware in den bestehenden Prototyp implementiert und können zukünftig zur effizienten, sicheren sowie automatisierten Bestimmung des Verhaltens einer Malware eingesetzt werden.