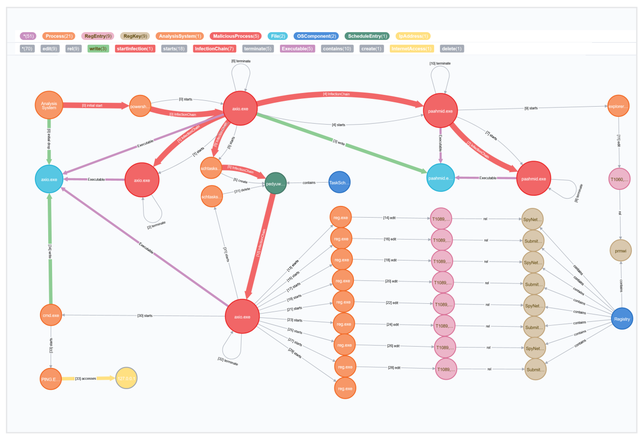
Westfälische Hochschule

Fachbereich Informatik & Kommunikation
Show & Tell 2021

Sysmon Sandbox Analysis Environment

Modul: Softwareprojekt (Master)

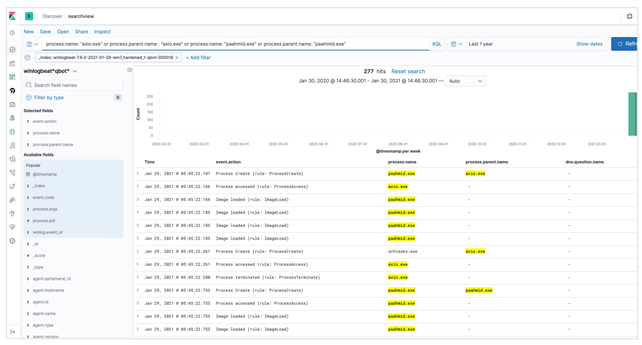
Team: Andreas Klopsch (IS), Alexander Schmitz (TI), Raphael Springer (IS)



Verhaltensgraph einer Qbot-Ausführung in neo4j

Problemstellung

Zur Erkennung von Malware kommen auf Endgeräten häufig Virenscanner zum Einsatz. Diese sind in der Lage bereits bekannte Malware auf Systemen zu erkennen und zu entfernen. Angriffe von feindlichen Akteuren werden jedoch immer raffinierter und herkömmliche Virenscanner reichen nicht mehr aus, um fortgeschrittene Angriffe zu erkennen. Um dem entgegen zu wirken, kommt in der Praxis Endpoint Detection and Response (EDR) zum Einsatz. Hierbei werden auf den Endgeräten sicherheitsrelevante Events gesammelt und an eine zentrale Instanz gesendet, welche mögliche Bedrohungen erkennt. Wir haben uns die Frage gestellt, ob wir anhand dieser sicherheitsrelevanten Events Malware-Familien erkennen können.

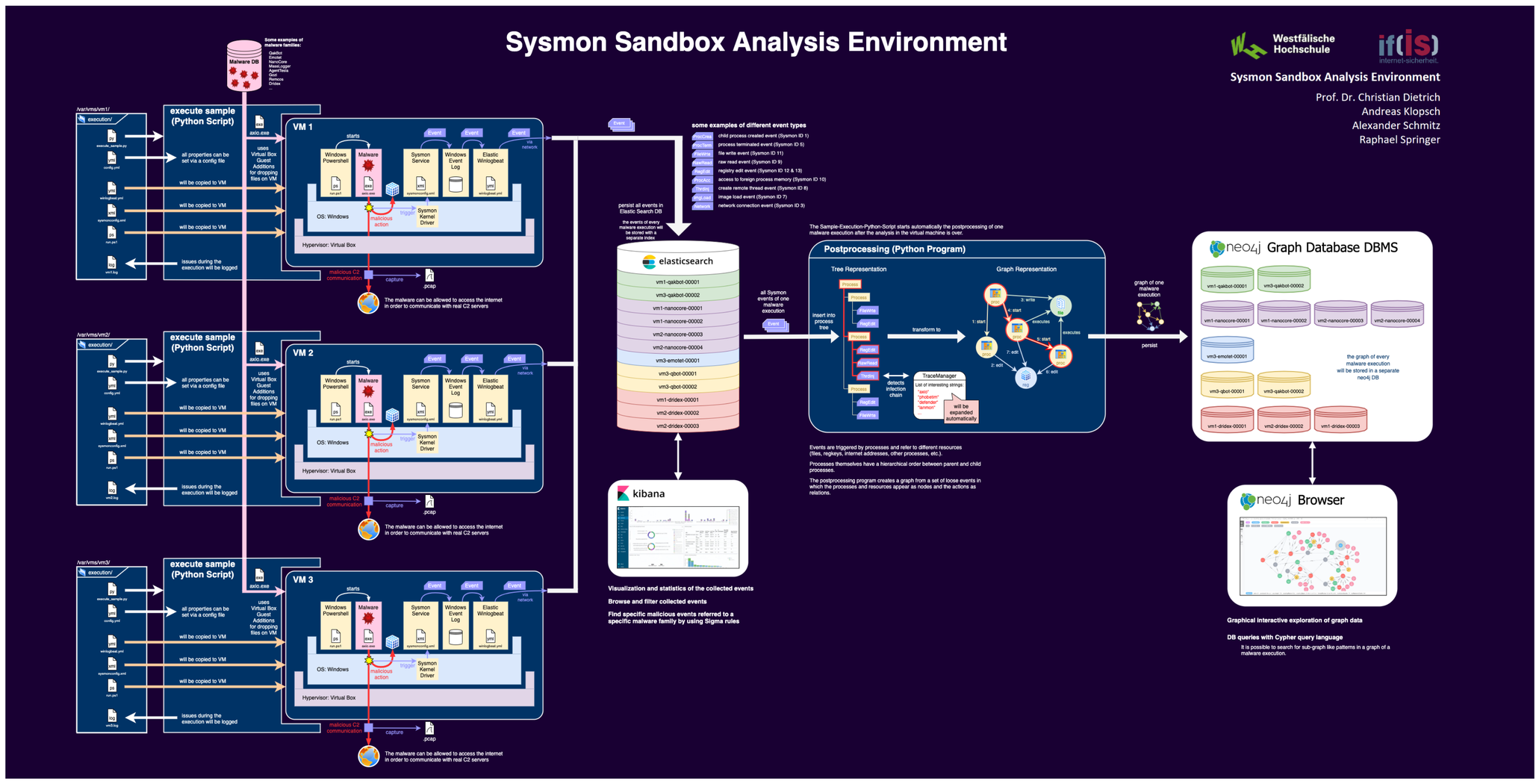


Ansicht einer Qbot-Ausführung in Kibana

Idee und Konzept

Unsere Idee war es eine Analyseumgebung zu bauen, mit welcher wir Malware ausführen, sicherheitsrelevante Events aggregieren und anschließend analysieren können. Hierzu haben wir virtuelle Maschinen als Endpunkte genutzt, in welchen Malware ausgeführt werden kann, ohne dass realer Schaden entsteht. Innerhalb der virtuellen Maschinen werden sicherheitsrelevante Events gesammelt und an ein Security Information and Event Management (SIEM) weitergeleitet. Dort können die Events geordnet und analysiert werden.

Technische Umsetzung



Team

klopsch@internet-sicherheit.de
schmitz@internet-sicherheit.de
springer@internet-sicherheit.de

Betreuung

Prof. Dr. Christian Dietrich, Fachgebiet: IT-Sicherheit