Analyse und Optimierung eines Obfuskators

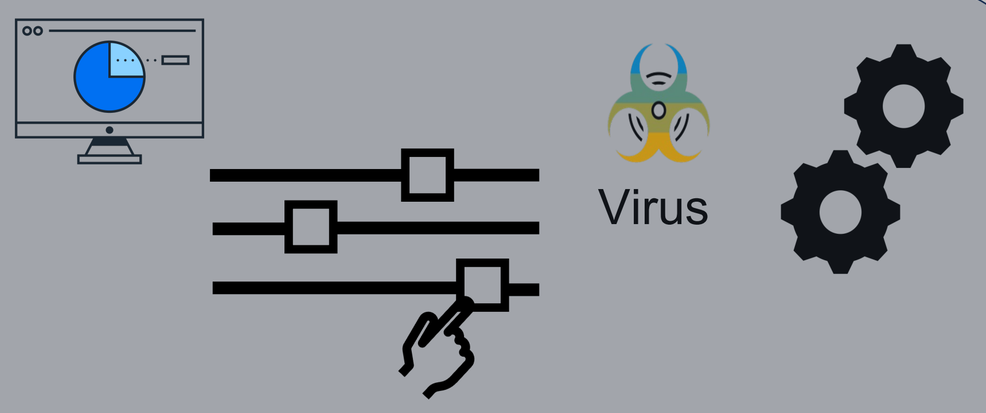
Johannes Wickles

1) Motivation

Ein Red Team ist eine Gruppe von Cybersecurity-Experten, die Sicherheitslücken in einem Unternehmen identifizieren und die Effizienz seiner Verteidigungsmaßnahmen testen. Dabei verwenden sie schädliche Programmcodes, die sogenannten Payloads, welche von Antiviren-Programmen unerkannt bleiben müssen, um ein realistisches Szenario eines echten Cyber-Angriffs zu simulieren. Dabei ist eine schnelle Herstellung solcher unentdeckter Payloads entscheidend.

Was ist ein Obfuskator?

Ein Obfuskator ändert den Quellcode von Programmen, um das Lesen und Verstehen zu erschweren und Virenerkennung zu behindern. Die dabei verwendeten Methoden beinhalten Umbenennungen von Variablen, unklare Programmierstrukturen, irrelevanten Code sowie Verschlüsselung.



2) Methodik

Mit dem Open-Source-Tool "Inceptor" kann man den Code in vielerlei Hinsicht verschleiern, z.B. durch Anpassung der Codestruktur und Verschlüsselung. Aber nicht jede Einstellung wirkt gegen jedes Antiviren-Programm gleich gut. Wir haben über 1000 unterschiedlich verschleierte Viren gegen verschiedene Antiviren-Programme getestet, um herauszufinden, welche Einstellungen am besten dabei helfen, den jeweiligen Virenschutz zu umgehen.

3) Ergebnisse

Die Analyse zeigt, welche Obfuskator-Kombinationen die besten Chancen haben, Antivirenprogramme zu überwinden. Wir konnten die Wahrscheinlichkeiten ermitteln, welche Kombination am besten gegen welches Programm funktioniert. So kann schneller eine unentdeckte Payload erzeugt werden. Bei Nutzung von zwei Antivirenprogrammen können wir durch Multiplikation die besten Kombinationen finden, indem wir annehmen, dass die Wahrscheinlichkeiten unabhängig sind. Dieser Ansatz skaliert gut, auch bei mehr als zwei Programmen.

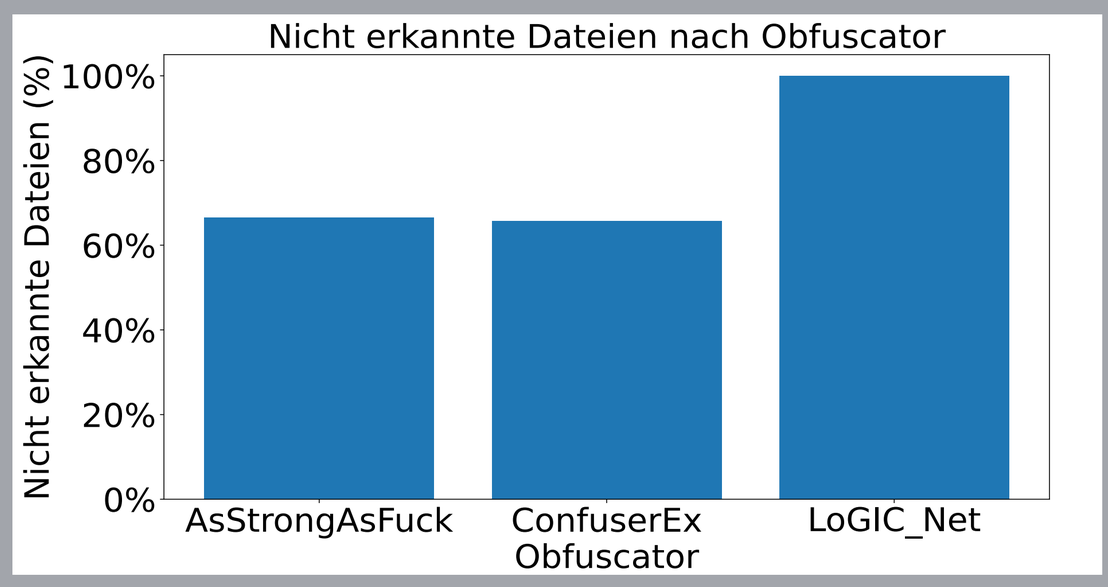


Abb. 1: Beispiel für die Analyse der Obfuskator gegen Windows Defender

4) Zusammenfassung

Basierend auf unseren Untersuchungsergebnissen haben wir ein Programm entwickelt, das die erfolgversprechendsten Inceptor-Konfigurationen nutzt. Diese variieren abhängig vom verwendeten Antiviren-Programm. Dadurch kann das Red Team effizienter Payloads erstellen, die vom Antiviren-Programm nicht erkannt werden. Das Tool beschleunigt deren Arbeit und lässt sich in automatisierte Prozesse einbauen.

h_da hochschule darmstadt informatik
member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Praxisprojekt 2
Informatik Dual
2024

Gruppe B