Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

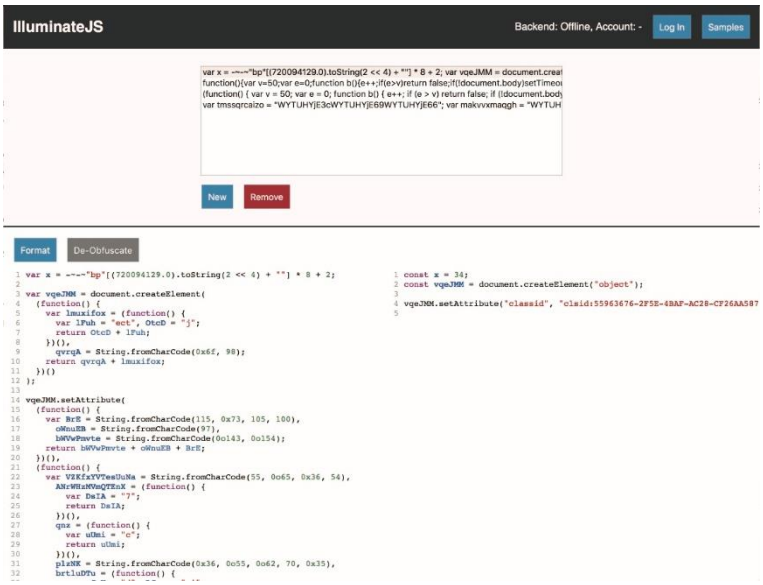
InIT Institut für angewandte
Informationstechnologie

Entschleierung von JavaScript mittels statischer Code-Analyse

Diplomand
Lucas Neiva

Dozent
Bernhard Tellenbach

"Obfuscation" ist ein englischer Begriff aus der Softwaretechnik. Er beschreibt die absichtliche Veränderung vom Programmcode mit dem Ziel, den ursprünglichen Quellcode zu verschleiern und in eine Form umzuwandeln, die schwieriger zu lesen, zu klassifizieren und zu analysieren ist. In der Praxis gibt es mindestens zwei Anwendungsfälle für das Verschleiern von Quellcodes: der Schutz von geistigem Eigentum und das Umgehen von signaturbasierten Anti-Malware-Programmen. Das Gegenstück zu den Verschleierungswerkzeugen stellen die Entschleierungswerkzeuge dar. Diese versuchen eine Verschleierung zumindest teilweise rückgängig zu machen, um z.B. die Analyse von einem Stück entsprechend präparierter Malware zu vereinfachen.
Diese Bachelor Arbeit analysiert das bekannte JavaScript Entschleierungswerkzeug JSDetox und macht insgesamt neun Vorschläge für eine Entschleierungsfunktionalität, die über dessen Fähigkeiten hinausgehen. Um die Verbesserungsvorschläge zu evaluieren, wurde ein auf Transformationen auf dem Abstract-Syntax-Tree (AST) basierendes Werkzeug entwickelt, das JavaScript partiell evaluiert und statisch vereinfacht. Die Ergebnisse der Evaluation zeigen, dass das Werkzeug mehr Informationen aus einem Stück JavaScript-Malware extrahieren kann als JSDetox.



Web-Interface welches zur Analyse verschleierter JavaScript-Malware verwendet werden kann.